Cognos® 8 Business Intelligence

ARCHITECTURE AND DEPLOYMENT GUIDE

COGNOS®

THE NEXT LEVEL OF PERFORMANCE™

Product Information

This document applies to Cognos® 8 Version 8.3 and may also apply to subsequent releases. To check for newer versions of this document, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

Copyright

Copyright © 2007 Cognos Incorporated.

Portions of Cognos® software products are protected by one or more of the following U.S. Patents: 6,609,123 B1; 6,611,838 B1; 6,662,188 B1; 6,728,697 B2; 6,741,982 B2; 6,763,520 B1; 6,768,995 B2; 6,782,378 B2; 6,847,973 B2; 6,907,428 B2; 6,853,375 B2; 6,986,135 B2; 6,995,768 B2; 7,062,479 B2; 7,072,822 B2; 7,111,007 B2; 7,130,822 B1; 7,155,398 B2; 7,171,425 B2; 7,185,016 B1;7,213,199 B2.

Cognos and the Cognos logo are trademarks of Cognos Incorporated in the United States and/or other countries. All other names are trademarks or registered trademarks of their respective companies.

While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Cognos does not accept responsibility for any kind of loss resulting from the use of information contained in this document.

This document shows the publication date. The information contained in this document is subject to change without notice. Any improvements or changes to either the product or the document will be documented in subsequent editions.

U.S. Government Restricted Rights. The software and accompanying materials are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to the restrictions in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (C)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48CFR52.227-19, as applicable. The Contractor is Cognos Corporation, 15 Wayside Road, Burlington, MA 01803.

This software/documentation contains proprietary information of Cognos Incorporated. All rights are reserved. Reverse engineering of this software is prohibited. No part of this software/documentation may be copied, photocopied, reproduced, stored in a retrieval system, transmitted in any form or by any means, or translated into another language without the prior written consent of Cognos Incorporated.

Table of Contents

Introduction 7

Part 1: Architecture

Chapter 1: Cognos 8 11

Chapter 2: The Multitiered Architecture 13
- User Interfaces 13
  - Web-based User Interfaces 14
  - Windows-based User Interfaces 17
- Tier 1. Web Server: Cognos 8 Gateways 18
- Tier 2. Applications: Cognos 8 Servers 19
  - Dispatcher 19
  - Content Manager 22
- Tier 3. Data: Content Providers 24
  - Content Store 24
  - Data Sources 25
  - Metric Store 26

Chapter 3: Communications 27
- Messaging and Dispatching 28
  - Local Preferred Dispatching 28
- Log Message Processing 28
  - Planning Log Message Destinations in a Distributed Installation 29
  - Recommendation -- Consolidate Log Messages in a Distributed Environment Using a Remote Log Server 30
  - Recommendation -- Configure a Log File for Each Log Server 31
- Database Connection Management 31
  - Content Store Database 31
  - Query Databases 32
  - Metric Store Databases 32
- Microsoft .NET Framework Interactions 32
- Port Usage 33
- Request Flow Processing 33
  - Accessing Cognos 8 34
  - Viewing a Report or Analysis 36
  - Running a Report or Analysis 36
  - Scheduling a Task to Run 38
  - Opening a Cognos Connection Folder 39
  - Running an Agent 40
- Portal Pages 41

Chapter 4: Workflow 43
- Planning for Implementation 44
- Installing Cognos 8 44

Configuring Cognos 8 45
Monitoring Configuration Changes 45
Configuring Security 46
Configuring Cognos 8 for Multilingual Reporting 46
Administering Cognos 8 47
Using Cognos 8 for Reporting and Analysis 47
Creating Reporting Models and Packages 48
Authoring Reports 49
Using Cognos 8 for Scorecarding 50
Packaging in Metric Studio 50
Authoring Scorecarding Applications 51
Using Cognos 8 to Create PowerCubes 51
Managing Events 52

Part 2: Deployment

Chapter 5: Implementation Planning Checklist 53

Chapter 6: Installation Options 55
Installing All Components on One Computer 55
Installing the Gateway on a Separate Computer 56
Installing Application Tier Components and Content Manager on Separate Computers 58
Multiple Installations of Content Manager 60
Modeling Tool Installation Options 61
Cognos 8 with Other Cognos Products 63
Cognos Products That Can Be Upgraded to Cognos 8 63
Cognos Series 7 Products That Can Be Migrated to Cognos 8 64
Cognos Products That Interoperate with Cognos 8 65
Cognos Series 7 Content That Can Be Recreated in Cognos 8 67

Chapter 7: Performance Planning 69
Capacity Planning 70
Estimating Cognos 8 User Load 70
Assessing Application Complexity 72
Planning Infrastructure Components 72
Scalability Planning 75
Web Server and Gateway Scalability 75
Cognos 8 Server Scalability 80
Availability Planning 81
Cognos 8 Gateway Availability 81
Cognos 8 Server Availability 82
Content Manager Availability 82
Content Store Availability 83

Chapter 8: Performance Monitoring and Tuning 85
Performance Metrics 85
Database Tuning 87
Application Server Tuning 87
Changing Memory Settings 87
Setting Connection Limits 87
Web Server Tuning 88

Cognos 8 Tuning 88
Designing Models and Reports for Performance 88
Tuning Cognos 8 Dispatchers 89
Tuning the Report Service, Batch Report Service, and Report Data Service 90
Setting Affinity Connections 90
Best Practices for Scheduled Reporting 92
Best Practices for Report Bursting 93
PDF Rendering 94
Low Bandwidth Connections 95
Disk Maintenance 95
Monitoring Cognos 8 Servers 95
Temporary Space for Cognos 8 Servers 95
Advanced Report Processing Configuration Settings 96

Chapter 9: Globalization Considerations 97
Locales 98
Adding Fonts to the Cognos 8 Environment 99
Changing the Language of the User Interface 100
Changing the Language of Reports, Data, or Metadata for Users 101
Customizing Currency, Numbers, Dates, and Times 103
Setting up a Multilingual Cognos 8 Environment 104
Configuring a Database for Multilingual Reporting 105

Part 3: Security

Chapter 10: Security Architecture 107
Cognos Application Firewall 107
Cognos Authentication Services 108
Cognos Namespace 108
Single Signon 109
Cognos Authorization Services 109
Distributed Administration 109
Permissions 109
Cryptographic Services 110
Using a Third-party Certificate Authority 110
Standard Cryptographic Provider 110
Enhanced Cryptographic Providers 111

Chapter 11: Securing the Deployment 113
Techniques for Securing the Operating System 114
Techniques for Securing the Network 118
Securing the Application 119
Recommendation - Use Cognos Application Firewall 119
Configuring the Cryptographic Environment 120
Securing Temporary Files 122
Techniques for Securing Access to Cognos Connection 123
Securing Cognos PowerCubes 127
Securing Data Source Signons 127
Securing the Content Store 128
Security Audit 128

Index 131

Introduction

This document is intended for use with Cognos 8.

This document is for the business intelligence solutions architect who oversees the setup, administration, and use of Cognos 8, a Web-based business intelligence solution with integrated reporting, analysis, scorecarding, and event management features.

Part 1 describes the Cognos 8 architecture from the perspectives of structure, communications, workflow, and security. Part 2 provides information to help you plan to install and configure Cognos 8 and to maximize its performance. Part 3 describes the Cognos 8 security architecture and provides guidelines for securing the deployment.

Audience

To use this guide effectively, you should already be familiar with your information technology infrastructure and with the business needs of the people in your organization who will use Cognos 8.

Related Documentation

Our documentation includes user guides, getting started guides, new features guides, readmes, and other materials to meet the needs of our varied audience. The following documents contain related information and may be referred to in this document.

Note: A Web page such as **The page cannot be found** may appear when clicking individual links in the following table. Documents are made available for your particular installation and translation configuration. If a link is unavailable, you can access the document on the Cognos Global Customer Services Web site (http://support.cognos.com). Logon credentials are available either from your administrator or by request from support.america@cognos.com.

Document	Description
Cognos 8 Installation and Configuration Guide	Installing, upgrading, configuring, and testing Cognos 8, changing application servers, and setting up samples
Cognos 8 Administration and Security Guide	Managing servers, security, reports, and portal services; setting up Cognos samples; troubleshooting; and customizing Cognos 8
Cognos 8 Getting Started	Teaching new users how to use Cognos 8
Framework Manager User Guide	Creating and publishing models using Framework Manager

Document	Description
Metric Studio User Guide	Authoring scorecard applications and monitoring the metrics within them
Report Studio Professional Authoring User Guide	Authoring reports that analyze corporate data according to specific needs
Query Studio User Guide	Creating self-service business intelligence reports
Analysis Studio User Guide	Exploring, analyzing, and comparing dimensional data
Event Studio User Guide	Creating and managing agents that monitor data and perform tasks when the data meets predefined thresholds
Cognos Configuration User Guide	Using Cognos Configuration to configure Cognos 8
Cognos Connection User Guide	Using Cognos Connection to publish, find, manage, organize, and view Cognos content, such as scorecards, reports, analyses, and agents
Cognos 8 Software Development Kit Developer Guide	Managing Cognos 8 processes and implementing custom reporting solutions by using a collection of cross-platform Web services, libraries, and programming interfaces provided with the Cognos 8 SDK
Cognos Enhanced Encryption Module for OpenSSL Installation and Configuration Guide	Installing and configuring the Cognos Enhanced Encryption Module for OpenSSL on Windows or UNIX
Cognos Enhanced Encryption Module for Entrust Installation and Configuration Guide	Installing and configuring the Cognos Enhanced Encryption Module for Entrust on Windows or UNIX

Finding Information

To find the most current product documentation, including all localized documentation, access the Cognos Global Customer Services Web site (http://support.cognos.com). Click the **Documentation** link to access documentation guides. Click the **Knowledge Base** link to access all documentation, technical papers, and multimedia materials.

Product documentation is available in online help from the **Help** menu or button in Cognos products. You can also download documentation in PDF format from the Cognos Global Customer Services Web site.

You can also read PDF versions of the product readme files and installation guides directly from Cognos product CDs.

Using Quick Tours

Quick tours are short online tutorials that illustrate key features in Cognos product components. To view a quick tour, start Cognos Connection and click the **Quick Tour** link in the lower-right corner of the Welcome page.

Getting Help

For more information about using this product or for technical assistance, visit the Cognos Global Customer Services Web site (http://support.cognos.com). This site provides product information, services, user forums, and a knowledge base of documentation and multimedia materials. To create a case, contact a support person, or to provide feedback, click the **Contact Us** link. For information about education and training, click the **Training** link.

Printing Copyright Material

You can print selected pages, a section, or the whole book. Cognos grants you a non-exclusive, non-transferable license to use, copy, and reproduce the copyright materials, in printed or electronic format, solely for the purpose of operating, maintaining, and providing internal training on Cognos software.

Chapter 1: Cognos 8

Cognos 8 is a solution designed to address the challenges of enterprise-scale reporting, analysis, scorecarding, and event notification.

The Cognos 8 architecture was designed for scalability, availability, and openness. It uses platform independent, industry proven technology, such as Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Web Services Definition Language (WSDL). For this reason, Cognos 8 can integrate with and leverage your existing technology infrastructure on multiple platforms.

The Cognos 8 architecture features a consistent, zero footprint, Web-based user interface for viewing, creating, and administering reports, analyses, scorecards, and events. It has a common dispatcher and supports leading relational databases as well as Online Analytical Processing (OLAP) and dimensionally modeled relational cubes. It ensures dynamic load balancing and provides failover recovery for 24 x 7 operation. It also provides a single point of administration, as well as Web-based delegated administration. Cognos 8 is fully open to third-party products and custom development. It also integrates with Web farms and supports multilingual reporting and scorecarding.

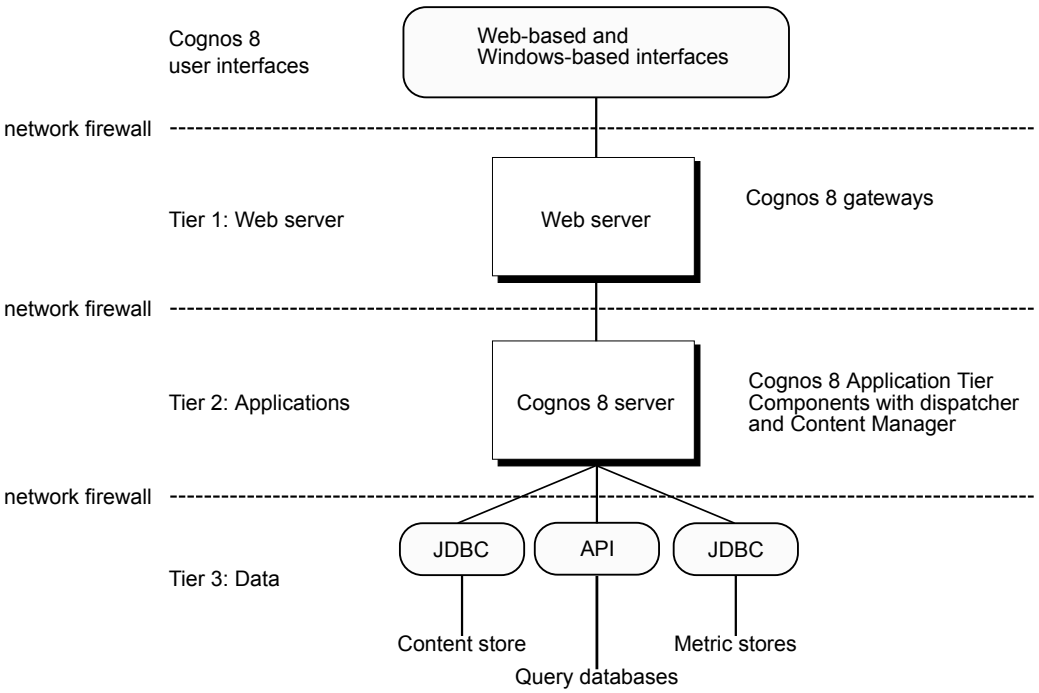
Cognos 8 Data Manager

Cognos 8 also includes Data Manager for data integration. With Data Manager, you can extract data from source systems and data files, transform the data, and load it into a data warehouse, conformed data mart, or report staging area.

For information about the Data Manager architecture, see the Data Manager *Installation and Configuration Guide* and the Data Manager *User Guide*.

Chapter 2: The Multitiered Architecture

Cognos 8 has a multitiered architecture. For description purposes, it can be separated into three tiers: Web server, applications, and data. The tiers are based on business function, and are typically separated by network firewalls. Cognos 8 user interfaces sit above the tiers.



This information describes a single-server Cognos 8 configuration. To meet your requirements, you can choose a different configuration. For more information, see "Installation Options" (p. 55).

User Interfaces

Cognos 8 is configured using Cognos Configuration. You also use Cognos Configuration to start and stop Cognos 8 services.

In addition to Cognos Configuration, Cognos 8 has Web-based and Windows-based user interfaces.

Web-based interfaces	Windows-based interfaces
Cognos Connection	Framework Manager
Cognos Administration	Metric Designer
Query Studio	Transformer
Report Studio	Map Manager

Web-based interfaces	Windows-based interfaces
Analysis Studio	Cognos 8 Go! Office
Event Studio	
Metric Studio	

Web-based User Interfaces

The zero footprint, Web-based interfaces include

- Cognos Connection (p. 14)
- Cognos Administration (p. 15)
- Query Studio (p. 16)
- Report Studio (p. 16)
- Analysis Studio (p. 16)
- Event Studio (p. 16)
- Metric Studio (p. 16)

The interfaces that are available to users depend on user permissions and on the Cognos 8 packages that your organization purchased.

Cognos Connection

Cognos Connection is a Web portal provided with Cognos 8, providing a single access point to the corporate data available for its products. It provides a single point of entry for querying, analyzing, and organizing data, and for creating reports, scorecards, and events. Users can run all their Web-based Cognos 8 applications through Cognos Connection. Other business intelligence applications, and URLs to other applications, can be integrated with Cognos Connection.

Like the other Web browser interfaces in Cognos 8, Cognos Connection uses the default configurations of your browser. It does not require the use of Java, ActiveX, or plug-ins, and does not install them.

In addition to selections for viewing data and creating objects, Cognos Connection includes

- portal pages

  The new page button opens a wizard where users can create a customizable page that uses portlets to show different types of content at the same time.

- Public Folders

  Public Folders store shared Cognos 8 content, such as packages (p. 48), reports, agents, shortcuts, and jobs.

- My Folders

  My Folders store personal Cognos 8 content, such as reports, shortcuts, and jobs.

- User preferences

  The my area button includes links to My Watch Items, alert lists and watch rules that help you monitor business events; My Preferences, settings for format, language, time zone, contact information, and portal content; and My Activities and Schedules, status windows where you can set priorities for and monitor your Cognos 8 activities.

- Link to tools and applications

  The **Launch** button provides links to the Cognos 8 studios, Drill-through Definitions, which are used to navigate through related data when querying or analyzing data, and Cognos Administration.

For information about using Cognos Connection, see the Cognos Connection *User Guide* or the online Quick Tour.

The open Cognos 8 architecture means that you can choose to integrate Cognos 8 into your organization's existing Web portal. You can use Portal Services, provided with Cognos 8, to integrate Cognos 8 with a number of portals, including

- SAP Enterprise
- IBM WebSphere
- Plumtree

For more information, see the *Administration and Security Guide*.

Cognos Administration

Cognos Administration is a central management interface that contains the administrative tasks for Cognos 8. It provides easy access to the overall management of the Cognos environment and is accessible through Cognos Connection.

Cognos Administration is organized into three sections:

- Status

  Use the links in this section to monitor activities, server status, and system metrics, and change some system settings.

- Security

  Use the links in this section to define users, groups, and roles for security purposes, configure capabilities for the interfaces and studios, and set properties for the user interface profiles (professional and express) that are used in Report Studio.

- Configuration

  Use the links in this section to set up data source connections, deploy Cognos 8 content from one content store (p. 24) to another, create distribution and contact lists, add printers, set styles,

manage portlets and portal layout, start or stop dispatchers and services, and change system settings.

For information about using Cognos Administration, see the *Administration and Security Guide*.

Query Studio

Query Studio lets users with little or no training quickly design, create and save reports to meet reporting needs not covered by the standard, professional reports created in Report Studio.

For information about using Query Studio, see the Query Studio *User Guide* or the online Quick Tour.

Report Studio

Report Studio lets report authors create, edit, and distribute a wide range of professional reports. They can also define corporate-standard report templates for use in Query Studio, and edit and modify reports created in Query Studio or Analysis Studio.

For information about using Report Studio, see the Report Studio *User Guide* or the online Quick Tour.

Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

For information about using Analysis Studio, see the Analysis Studio *User Guide* or the online Quick Tour.

Event Studio

In Event Studio, you set up agents to monitor your data and perform tasks when business events or exceptional conditions occur in your data that must be dealt with. When an event occurs, people are alerted to take action. Agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events. For example, a support call from a key customer or the cancellation of a large order may trigger an event, sending an email to the appropriate people.

For information about using Event Studio, see the Event Studio *User Guide* or the online Quick Tour.

Metric Studio

In Metric Studio, you can create and deliver a customized scorecarding environment for monitoring and analyzing metrics throughout your organization. Users can monitor, analyze, and report on time-critical information by using scorecards based on cross-functional metrics.

For information about using Metric Studio, see the Metric Studio *User Guide for Authors*.

Windows-based User Interfaces

The Windows-based Cognos 8 interfaces are the modeling components: Framework Manager, Metric Designer, Transformer, and Map Manager.

Framework Manager

Framework Manager is the Cognos 8 modeling tool for creating and managing business-related metadata for use in Cognos 8 analysis and reporting. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

OLAP cubes are designed to contain sufficient metadata for business intelligence reporting and analysis. Because cube metadata may change as a cube is developed, Framework Manager models the minimum amount of information needed to connect to a cube. Cube dimensions, hierarchies, and levels are loaded at run time.

For information about using Framework Manager, see the Framework Manager *User Guide*.

Metric Designer

Metric Designer is the Cognos 8 modeling tool used to create extracts for use in Cognos 8 scorecarding applications. Extracts are used to map and transfer information from existing metadata sources such as Framework Manager and Impromptu Query Definition (.iqd) files.

For information about using Metric Designer, see the Metric Designer *User Guide*.

Cognos 8 Go! Office

Cognos 8 Go! Office allows users to access Cognos reporting data directly within Microsoft Office applications.

Cognos 8 Go! Office makes use of the Microsoft .NET Framework to allow clients to interact with server-based components. Cognos 8 Go! Office provide two types of clients:

- The smart client provides a zero-administration client with a zero-deployment impact. Product updates are automatically captures though the smart client.
- The COM add-in client requires a client installation. Product updates are delivered by uninstalling and reinstalling the COM add-in client.

For more information about using Cognos 8 Go! Office, see the Cognos 8 Go! Office *User Guide*. For more information about configuring and deploying Cognos 8 Go! Office clients, see the *Installation and Configuration Guide*.

Transformer

Cognos 8 Transformer is the Cognos 8 modeling tool used to create PowerCubes for use in Cognos 8. Secured Cognos 8 PowerCubes are not compatible with Cognos Series 7.

For information about installing and configuring versions of Transformer that are earlier than 8.3, see the documentation provided with your edition of Transformer.

Map Manager

Administrators and modelers use a Windows utility named Map Manager to import maps and update labels for maps in Report Studio. For map features such as country and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

For information about using Map Manager, see the Map Manager *Installation and User Guide*.

Tier 1. Web Server: Cognos 8 Gateways

The Cognos 8 Web server tier contains one or more Cognos 8 gateways.

Web communication in Cognos 8 is typically through gateways, which reside on one or more Web servers. A gateway is an extension of a Web server program that transfers information from the Web server to another server.

Web communication can also occur directly with a Cognos 8 dispatcher (p. 19), although this option is less common than using gateways.

If you install the gateway component on a different computer from Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher, preferably one on an Application Tier Components computer. For failover protection, you can configure more than one dispatcher for a gateway computer (p. 19).

Cognos 8 supports several types of Web gateways, including

- CGI

  The default gateway, CGI can be used for all supported Web servers. However, for enhanced performance or throughput, you may choose one of the other supported gateway types.

- ISAPI

  ISAPI can be used for the Microsoft Internet Information Services (IIS) Web server. It delivers faster performance for IIS.

- apache_mod

  You can use an apache_mod gateway with the Apache Web server.

- servlet

  If your Web server infrastructure supports servlets or you are using an application server, you can use a servlet gateway.

When a Cognos 8 gateway receives a request, it

- encrypts passwords to ensure security
- extracts information needed to submit the request to a Cognos 8 server
- attaches environment variables for the Web server
- adds a default namespace to the request to ensure that the server authenticates the user in the correct namespace

- passes requests to a Cognos 8 dispatcher for processing

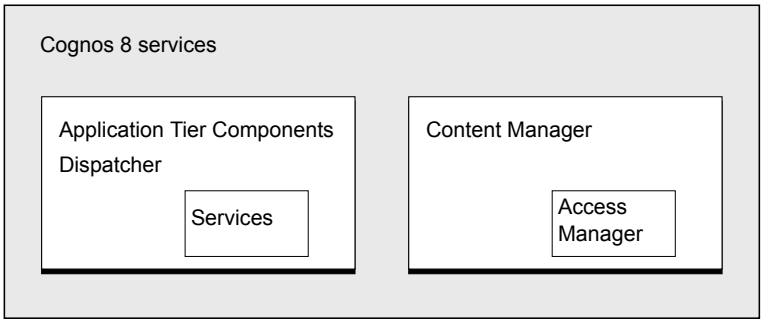
For information about configuring Cognos 8 gateways, see the *Installation and Configuration Guide*.

Tier 2. Applications: Cognos 8 Servers

The Cognos 8 applications tier contains one or more Cognos 8 servers. A Cognos 8 server runs requests, such as reports, analyses, and queries, that are forwarded by a gateway. A Cognos 8 server also renders the Cognos Connection and Metric Studio interfaces.

Each Cognos 8 installation includes

- Application Tier Components, which include a dispatcher (p. 19), that operates services and routes requests
- Content Manager (p. 22), which manages Cognos 8 information



Dispatcher

The dispatcher starts all Cognos 8 services configured and enabled on a computer, and routes requests. The dispatcher is a multithreaded application that uses one or more threads per request. Configuration changes are routinely communicated to all running dispatchers. The dispatcher includes Cognos Application Firewall to provide security for Cognos 8. For more information, see "Cognos Application Firewall" (p. 107).

The dispatcher can route requests to a local service, such as the report service, presentation service, job service, or monitor service.

A dispatcher can also route requests to a specific dispatcher to run a given request. Requests can be routed to specific dispatchers based on load-balancing needs, or package or user group requirements. For example, if a particular OLAP data source is available for only one Cognos server group, you specify that all requests for the data source be routed to that Cognos server group. For more information about routing requests based on packages or user groups, see the *Administration and Security Guide*.

When you configure Cognos 8 gateways, you can list the universal resource identifiers (URIs) of target dispatchers in order of most to least preferred. If a dispatcher fails, requests are routed to another dispatcher based on the list. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service. For more information, see the *Installation and Configuration Guide*.

When a dispatcher starts, it registers itself with Content Manager. As a result, each dispatcher is aware of the other dispatchers. If a dispatcher fails or is unavailable, requests for that dispatcher are routed to the next available dispatcher until the failed dispatcher reregisters itself.

Cognos 8 Services

After you install and configure Cognos 8, one dispatcher is available on each computer by default. Each dispatcher has a set of associated services, listed in the following table.

Service	Purpose
Agent service	Runs agents. If the conditions for an agent are met when the agent runs, the agent service asks the monitor service to run the tasks.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitor service.
Content Manager service	• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy • Performs content store management functions, such as import and export
Data movement service	Manages the execution of data movement tasks in Cognos 8. Data movement tasks, such as Builds and JobStreams, are created in Data Manager Designer and published to Cognos 8.
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, agent service, or data integration service
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics
Job service	Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.

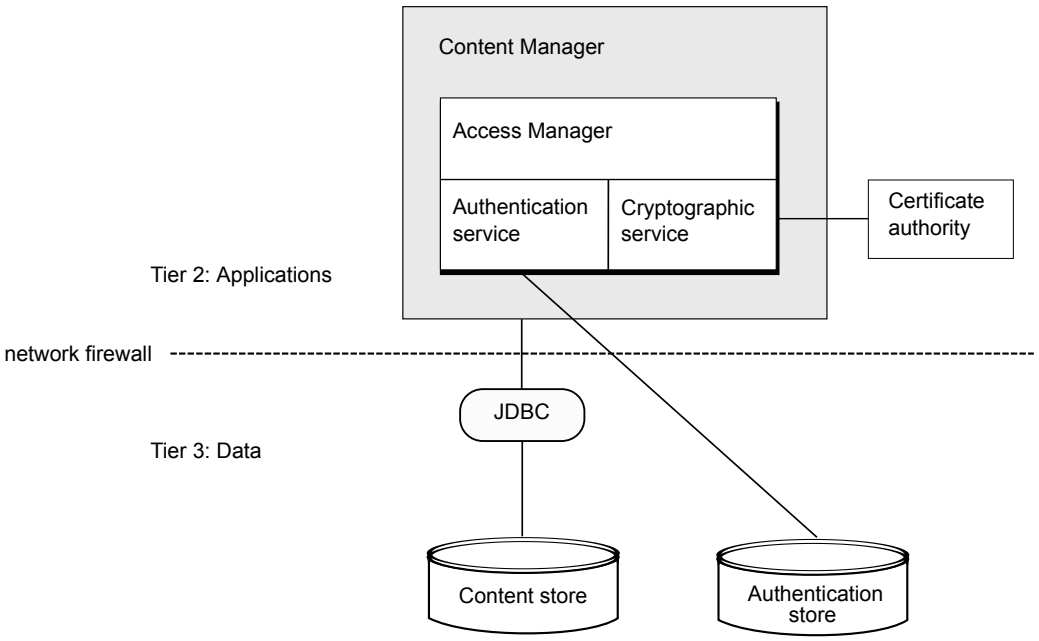
Service	Purpose
Log service	Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Customer Support, including: • security events • system and application error information • selected diagnostic information
Metric Studio service	Provides the Metric Studio user interface for monitoring and entering performance information
Migration service	Manages the migration from Cognos Series 7 to Cognos 8.
Monitor service	• Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task • Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent. • Creates history objects within the content manager and manages failover and recovery for executing entries
Planning job service	Manages communications with the Planning Job Server subsystem.
Planning web service	Manages communications with Contributor Web and Contributor Add-in for *Excel* users.
Planning administration console service	Manages communication with the Contributor Administration Console.
Planning data service	Manages communications for real-time reporting from Contributor plan data in Cognos 8.

Service	Purpose
Presentation service	• Transforms generic XML responses from another service into output format, such as HTML or PDF • Provides display, navigation, and administration capabilities in Cognos Connection
Report data service	Manages the transfer of report data between Cognos 8 and applications that consume the data, such as Cognos 8 Go! Office and Cognos 8 Go! Mobile.
Report service	Manages interactive requests to run reports and provides output for a user in Cognos Connection or a studio
System service	Defines the Business Intelligence Bus API-compliant service used to obtain application-wide Cognos 8 configuration parameters. It also provides methods that normalize and validate locale strings and map locale strings to locales supported by your application.

Content Manager

Content Manager is the Cognos 8 service that manages the storage of customer application data, including security, configuration data, models, metrics, report specifications, and report output. Content Manager is needed to publish models, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store (p. 24) database, which is typically located in Tier 3 of the architecture.



Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby. The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

Although we describe Content Manager as part of the applications tier, for maximum security you can choose to configure Cognos 8 with Content Manager in the data tier.

The information stored by Content Manager includes

- reports

  Reports contain specifications, properties, security settings, and outputs. This includes analyses created in Analysis Studio, queries created in Query Studio, and reports created in Report Studio.

- report packages

  Packages contain metadata, reports, and folders.

- metric packages

  Metric packages contain metadata, scorecards, and folders.

- agents

  Agents include the conditions, schedules, and tasks used to monitor events and deliver notifications. This includes the list of recently detected instances of an event.

- server configuration

  Server configuration contains directory information, the Cognos namespace (p. 108), and information about contacts, distribution lists, data sources, and printers.

- personal user information

  Personal user information consists of My Folders and My Pages.

- language information

  Language information includes names, descriptions, and tool tips in different languages to support Cognos 8 multilingual capabilities.

Content Manager performs general functions, such as add, query, update, delete, move, and copy. It also performs content store management functions, such as export and import.

Access Manager

Content Manager contains Access Manager, the primary security component of Cognos 8. Access Manager leverages your existing security providers for use with Cognos 8. It provides Cognos 8 with a consistent set of security capabilities and APIs, including user authentication (p. 108), authorization (p. 109), and encryption (p. 110). It also provides support for the Cognos namespace (p. 108).

Some security capabilities, such as user authentication, are external to Cognos 8 but are exposed to Cognos 8 by Access Manager. Other capabilities, such as authorization, are internal to Cognos 8, and are implemented by Access Manager.

For many security-related functions, Access Manager requires certificates, and interacts with a certificate authority. By default, Cognos 8 uses its own certificate authority service to establish the root of trust in the Cognos 8 security infrastructure. If you use a third-party certificate authority, you can configure Cognos 8 to use it instead of the default Cognos 8 certificate authority. For more information, see "Security Architecture" (p. 107).

Tier 3. Data: Content Providers

The Cognos 8 data tier contains the

- content store (p. 24)
- data sources (p. 25)
- metric store (p. 26)

Content Store

The content store is a relational database that contains data that Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the Cognos namespace itself; and information about scheduling and bursting reports. The relational database can be Cognos Content Database or a database from a supported third-party vendor.

Design models and log files are not stored in the content store.

Cognos 8 includes the Cognos Content Database as a default content store. You can use the Cognos Content Database as your content store, or you can use other databases, such as Microsoft SQL Server, Oracle, IBM DB2, or Sybase.

The Cognos 8 service that uses the content store is named Content Manager.

Content Manager uses a JDBC (Java DataBase Connectivity) API to access the content store and metric stores. Cognos 8 comes with the JDBC drivers for Cognos Content Database and MS SQL Server. Oracle, IBM, and Sybase JDBC drivers, which are required for their respective databases, are available from their vendors.

Cognos does not publish the content store schema, but updates the schema periodically, isolating changes from the user through stable user interfaces and APIs.

Much of the information in the content store, such as report results and XML report specifications, is stored as binary large object (BLOB) fields.

PDF results are compressed from creation, to storage, to serving, to the browser. The PDF format does not allow the main body of a report to be compressed, but the page contents, fonts, and images are compressed. Adobe Acrobat Reader uncompresses PDF files at view time.

Report results in other formats, such as HTML, XML, and CSV (comma separated values), are stored in compressed form and are uncompressed by Content Manager before they are sent to a user.

Cognos Content Database

Cognos Content Database is an instance of an Apache Derby database that can be optionally installed and used as the default content store. Cognos Content Database can be used where you do not want to implement a commercial database for the content store.

Apache Derby is open source software whose license terms can be found on the Apache Derby Web site (http://db.apache.org/derby/license.html). Any modifications to the Apache Derby database, and its use with other than Cognos products is not supported by Cognos. Any modifications you make to the Apache Derby database are at your own risk.

Cognos Content Database can be installed with other Cognos 8 components or installed on a separate computer. The Cognos Content Database service starts the Apache Derby database in which the Cognos Content Database is running.

If you install Cognos Content Database on the same computer as Content Manager, Cognos Content Database will be used as the default content store. For information about changing your content store, see the *Installation and Configuration Guide*.

Data Sources

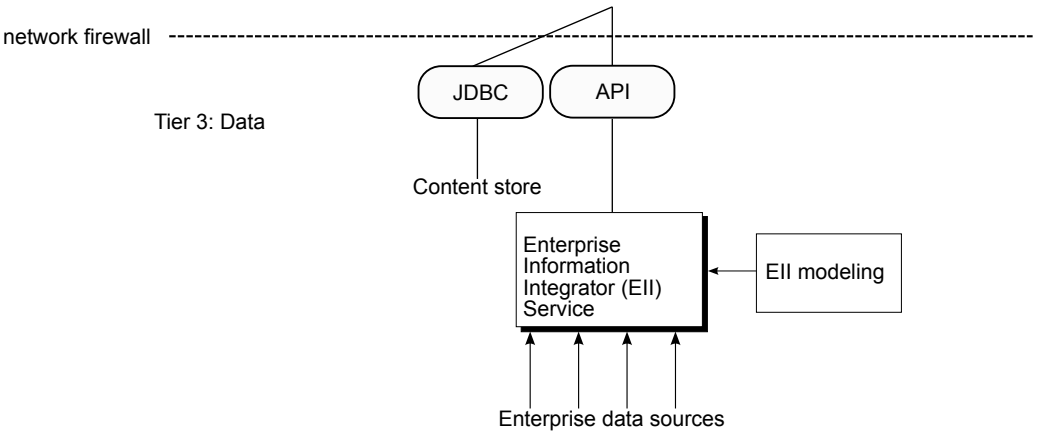
Data sources, also known as query databases, are relational databases, dimensional cubes, files, or other physical data stores that can be accessed through Cognos 8. Application Tier Components use data source connections to access data sources.

Enterprise Information Integrators

Cognos 8 can be used with Enterprise Information Integration (EII) products such as the Composite Information Server.

Composite Information Server provides access to additional data sources such as LDAP, JDBC, Open XML and WSDL, and improves performance when querying data from different data sources.

In the following scenario, the EII product models a set of databases, producing a unified view as a single virtual data source. Cognos 8 accesses the EII service as though it were a single database, and the EII service joins data from the various enterprise data sources as needed.



Metric Store

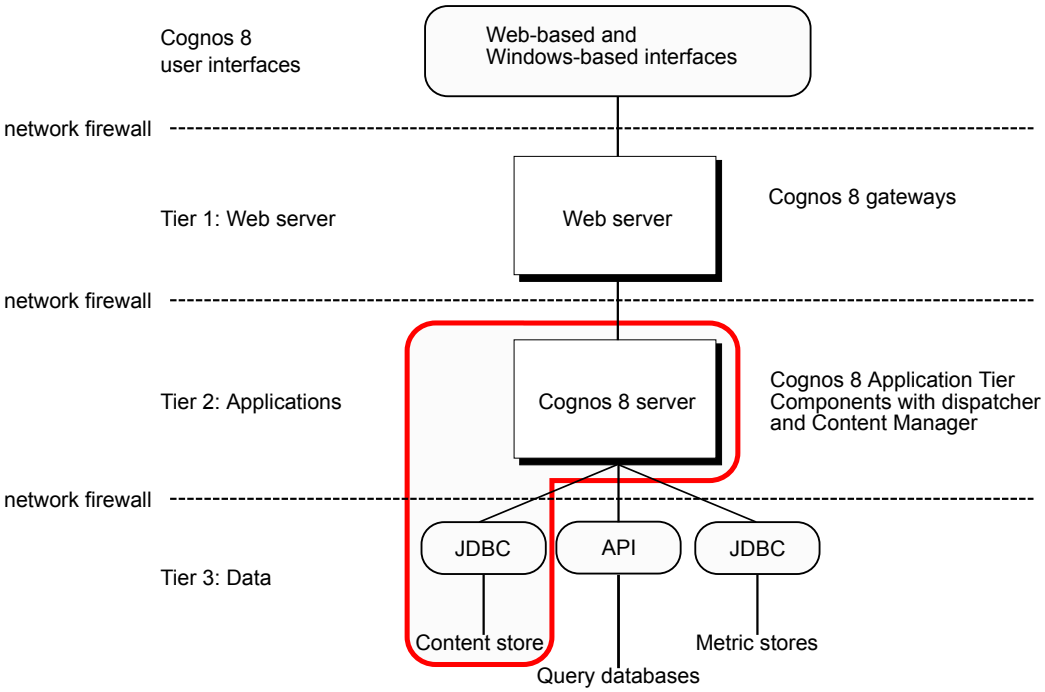
A metric store is a relational database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

More than one metric store may be created. For example, one metric store may contain content for a sales application and another metric store may contain content for a finance application.

Chapter 3: Communications

Cognos 8 components communicate with each other, and with any additional applications integrated with Cognos 8, using the BI Bus. The BI Bus is an open, documented, Simple Object Access Protocol (SOAP) API that supports Web Services Definition Language (WSDL). For information about integrating applications with Cognos 8 components, see the Cognos 8 Software Development Kit *Developer Guide*.

The BI Bus is not a software component like Content Manager or a Cognos 8 server, but a set of protocols that govern communications among Cognos 8 services. It also defines how third-party industry standards and protocols are used with Cognos 8, enabling Cognos 8 to be a fully open system.



Everything that is managed through Cognos Connection (p. 14) or your third-party portal is exposed through the BI Bus. This includes packages, folders, reports, analyses, events, directory objects, servers, deployment objects, and metadata. Using an API through the Cognos 8 SDK, you can create, read, update, and delete these objects, and set security and other properties.

The processes enabled by the BI Bus protocol include

- messaging and dispatching
- log message processing
- database connection management
- Microsoft .NET Framework interactions
- port usage

- request flow processing
- portal pages

Messaging and Dispatching

The Cognos 8 architecture is tuned to minimize dispatch time. Cognos 8 can use network capabilities, such as load-balancing routers, to ensure that dispatchers and Web gateways are used evenly. Load-balancing routers distribute requests across multiple Web or application servers, ensuring that all dispatchers share the workload.

The dispatcher load-balancing scheme is a static algorithm. You can specify a weight for each dispatcher. A dispatcher with a weight of 2 can do twice the work of a dispatcher with a weight of 1, and so on. Each dispatcher spreads work among all the dispatchers using a weighted round-robin algorithm.

Local Preferred Dispatching

When using any sort of external load-balancing mechanism, you should use the local preferred dispatch option. By using this option, the dispatcher does not perform load balancing. Requests that can be processed locally will be processed locally. If the external load balancing mechanism sends a request to a computer on which the required service is not available, the dispatcher routes the request to an appropriate computer.

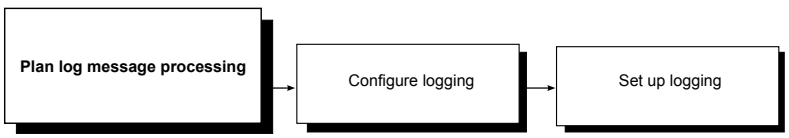
For more information, see "Load Balancing" (p. 75).

Log Message Processing

Log messages are an important diagnostic tool for investigating the behavior of Cognos 8. In addition to error messages, log messages provide information about the status of components and a high-level view of important events. For example, log messages can provide information about attempts to start and stop services, completion of processing requests, and indicators for fatal errors. Audit logs, which are available from a logging database, provide information about user and report activity.

The Cognos 8 services on each computer send information about errors and events to a local log server. A local log server is installed in the *c8_location*/logs folder on every Cognos 8 computer that contains Content Manager or Application Tier Components. Because the log server uses a different port from the other Cognos 8 components, it continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

The following workflow shows the tasks that are required to prepare for logging.

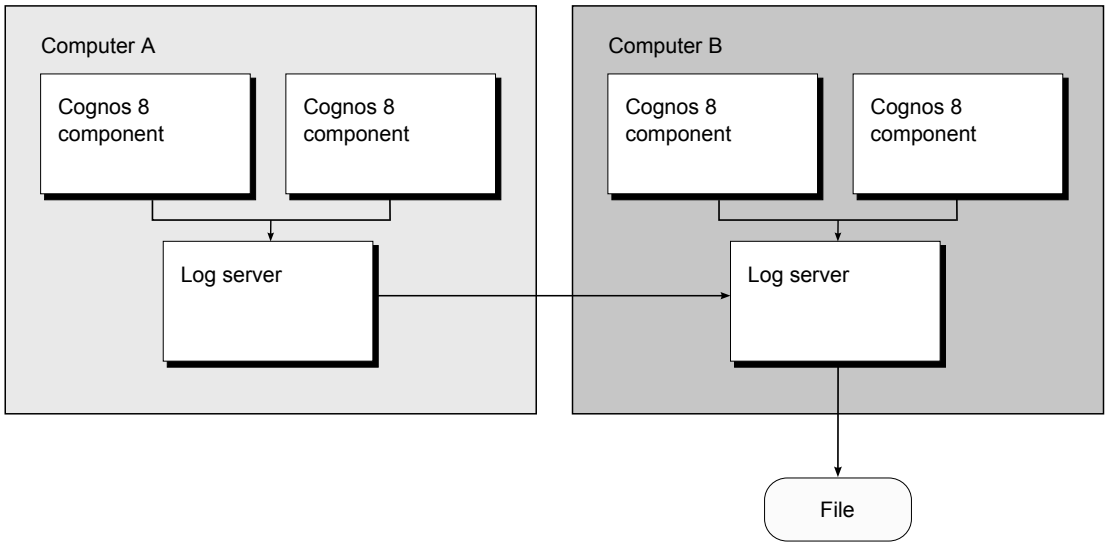


- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message destinations, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a third-party database. Consider security, such as methods available for protecting log files from system failures and user tampering. For information about planning, see the *Architecture and Deployment Guide*.
- During configuration, define the startup properties for logging, such as connection settings for third-party databases. You must also create a logging database if you plan to collect audit logs. If communication between a local log server and a remote log server must be secured, make the appropriate configuration changes on both Cognos 8 computers. For information about configuring logging, see the *Installation and Configuration Guide*.
- When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity. For information about setting up logging, see the *Administration and Security Guide*.

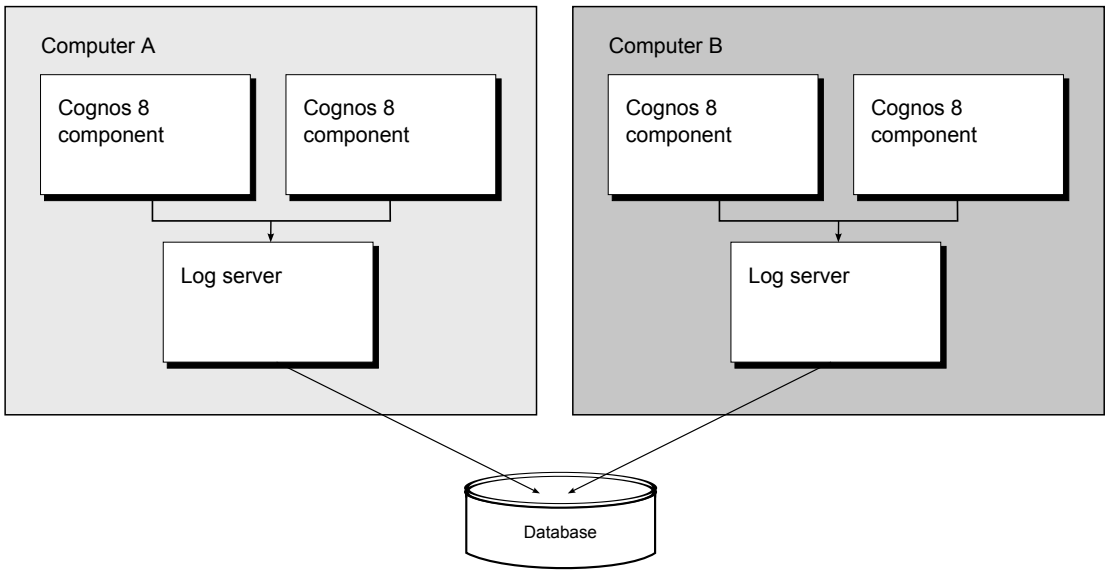
For information about using log messages to solve problems and resolving logging-related issues, see the Troubleshooting section of the *Administration and Security Guide*.

Planning Log Message Destinations in a Distributed Installation

Distributed installations of Cognos 8 have more than one log server. With distributed installations, you can send log information to a central location. For example, you can configure Cognos 8 to send log information to a common log server. This log server sends the log information to a single destination on the same or a different computer.



You can also configure Cognos 8 to send audit log information from each log server to a common database. The common database can be on the same computer as one of the log servers, or on a different computer.



The local log server provides failover and recovery processes in the following three circumstances:

- When the local log server is configured to send log information to a remote log server that is not available, log information from the local log server is stored in local recovery files. When the remote log server becomes available, an automatic recovery process moves information from the local recovery files to the remote log server, and deletes the local recovery files.
- When local Cognos 8 components are configured to communicate with the local log server using a TCP connection and this connection is not available, log information for these local components is stored in local recovery files. When the TCP connection becomes available, an automatic recovery process moves information from the local recovery files to the remote log server, and deletes the local recovery files.
- When a log server is configured to send audit log information to a database, and the connection between the log server and the database fails, no information is logged in the database. When the connection is restored, information about the connection failure and restoration is stored in the local log file, if it exists, and the log server resumes sending new log information to the database. This information stored in the local log file is not stored in the logging database.

For information about specifying where to send log messages and configuring TCP connections, see the *Installation and Configuration Guide*.

Recommendation -- Consolidate Log Messages in a Distributed Environment Using a Remote Log Server

In a default configuration, the local log server on each Content Manager or Application Tier Components computer writes log messages to a local file. Configurations that consolidate the contents of individual log files may improve usability and performance.

Consider consolidating log messages produced on each Cognos 8 computer by sending them to a remote log server. Configure the remote log server to send all messages to a single log file or to send audit logs to a database (p. 29).

Log messages may be easier to interpret if all messages from each Cognos 8 computer appear in a consolidated location. For example, the log messages can then be sorted by their timestamp to determine the order in which events on various Cognos 8 computers occurred.

If you are using a database to capture audit log messages, performance may be improved if you route all audit log messages to a single log server that sends messages to the database. If a single log server is not used, the local log server on each Cognos 8 computer would require its own connection to the database.

Another benefit of using a single log server with a database is that configuration changes to the database are easier to maintain. You must update the configuration of only the remote log server.

Recommendation -- Configure a Log File for Each Log Server

We recommend that you configure a log file for each remote log server. Log files can provide important diagnostic and backup information if a communication issue occurs between a log server and the log message destination. For example, the TCP/IP connection between a local log server and a remote log server may become unavailable or a logging database may fail.

For local log servers, we recommend that you do not remove the default log files, even if you specify another destination for log messages, such as a database or remote log server. If the log messages may contain sensitive information, ensure that the log files on each computer are secured appropriately.

If a communication issue occurs, the local log server writes the log messages that it receives to the local log file. This action means that log messages are not lost when they cannot be written to a destination that is no longer available. As well, the log server writes information to the log file about the communication issue, which may help diagnose the problem. For example, if a database becomes unavailable, the log file contains information about when it failed, as well as when it recovered, if applicable.

Database Connection Management

Cognos 8 uses databases for several purposes: content store database, query database, or metric store database.

For some types of databases, such as Oracle, API client software must be installed and configured on each Cognos 8 server.

Content Store Database

The Content Manager service accesses the content store. Content Manager uses one database connection per request. Content Manager creates new database connections as required, pools connections, and reuses existing connections when possible. Content Manager maintains all database connections for the duration of the Content Manager operation. The theoretical maximum number of concurrent Content Manager requests equals the number of requests accepted by the Java application server or Tomcat.

When other Cognos 8 services are on the same computer as Content Manager, requests may be divided between Content Manager and the other services. In this case, the number of connections available to Content Manager may be fewer than the maximum possible connections.

Query Databases

The Cognos 8 server computer accesses the query databases. You can configure the maximum number of query database connections available to the Cognos 8 server computer, and the duration that connections are retained. A cleanup thread examines the connections every minute. Any connection that has been inactive longer than the time-out value is removed.

Inactive query database connections can be claimed by a new request. This occurs when the maximum number of connections has been reached and none of the inactive connections can be used by the new request. In this case, the oldest inactive connection is terminated and a new connection is created. A query database connection is only reused when the database credentials of the connection match those of the new request.

If the maximum number of connections is reached, and all are active, additional requests fail.

Metric Store Databases

A metric store database is a special case of a query database. A metric store database is used to store the information associated with metrics that appear in scorecards, including

- targets
- performance metrics
- thresholds
- membership in scorecards
- links to related reports, initiatives, and counter measures

Metric Studio accesses the metric store database. Metric Designer is used to define jobs that extract data from other query databases and populate the metric store database, although you can also manually create processes to do this.

Microsoft .NET Framework Interactions

Microsoft .NET Framework allows managed-code applications to interact with server-based applications through the use of Web services. Cognos 8 uses Microsoft .NET Framework to enable users' computers to interact with Cognos 8 server components for access to Cognos 8 Go! Office and its features.

Cognos 8 Go! Office is a managed-code application that takes advantage of the Microsoft .NET Framework. Cognos 8 Go! Office functions like a Microsoft Office plug-in, but is installed, configured, and deployed as a managed-code application.

Cognos 8 Go! Office uses Microsoft .NET Framework to allow users to interact with server-based components. Microsoft .NET Framework and the required updates are downloaded and installed

by the setup file when you install Cognos 8 Go! Office. The setup file must be run on all user computers.

For a list of supported versions of Microsoft .NET Framework, view the Cognos Global Customer Services Web site (http://support.cognos.com).

The Microsoft .NET Framework does not have to be installed on your Cognos 8 server. Cognos 8 Go! Office can run on any supported Cognos 8 server platform.

For information about configuring Cognos 8 Go! Office, see the *Installation and Configuration Guide*.

Port Usage

All communication between Cognos 8 components, except for Cognos Content Database and log server communication, can take place through one incoming port. This is true whether components are on the same computer or on different computers and whether communication is all non-SSL protocol or all SSL protocol. The default port number is 9300.

If Cognos 8 is configured to use a combination of non-SSL protocol and SSL protocol, communication takes place through two ports. You can use the default port for the non-SSL protocol communication and use a different port, such as 9334, for the SSL protocol communication.

Log server communication must take place through a unique port. The default port is 9362. You can configure log server communication to use either non-SSL or SSL protocol.

Framework Manager, Metric Designer, and Cognos 8 Transformer can communicate with the Cognos 8 server using either of two routes: through the Web server gateway, or directly to the Application Tier Components dispatcher. For more information see "Modeling Tool Installation Options " (p. 61).

Communications with third-party software products, such as databases and authentication providers, use the ports required by those products.

For information about using SSL and specifying where to send log messages, see the *Installation and Configuration Guide*.

Request Flow Processing

Request flow describes internal Cognos 8 responses to user requests. In general, browser requests go through the Cognos 8 Web gateway (p. 18) and are sent to a dispatcher. Before any processing is performed by the dispatcher, the request is validated by Cognos Application Firewall. A passport is attached to each request as a record of a valid user session.

Simple Object Access Protocol (SOAP) requests can be directed to either the Cognos 8 Web gateway or the dispatcher. For more information, see the *Installation and Configuration Guide*.

There are hundreds of types of requests and responses in Cognos 8. To illustrate request flow, this section describes how Cognos 8 responds to a request:

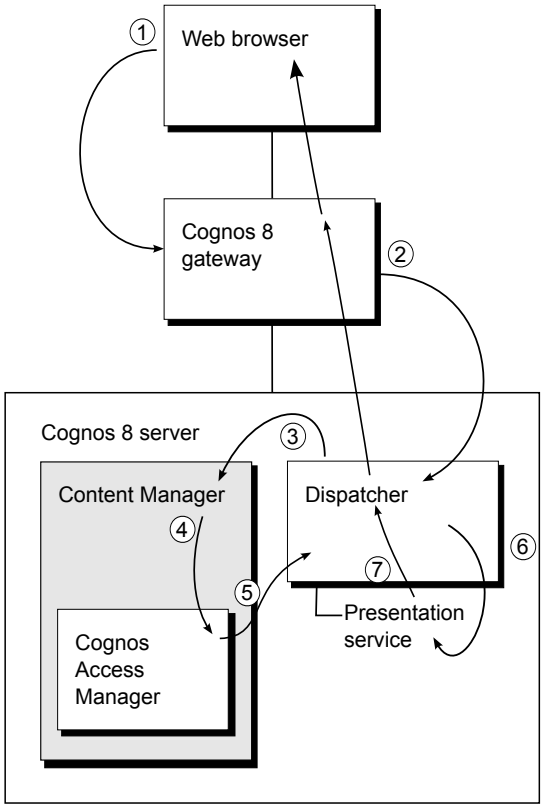
- to access Cognos 8 (p. 34)

- to view a report or analysis (p. 36)
- to run a report or analysis (p. 36)
- to run a scheduled task (p. 38)
- to open a Cognos Connection folder (p. 39)
- to run an agent (p. 40)

Accessing Cognos 8

A user can request anonymous or authenticated access to Cognos 8. Anonymous access can be enabled or disabled for Cognos 8. For more information see "Cognos Authentication Services" (p. 108).

Anonymous Access

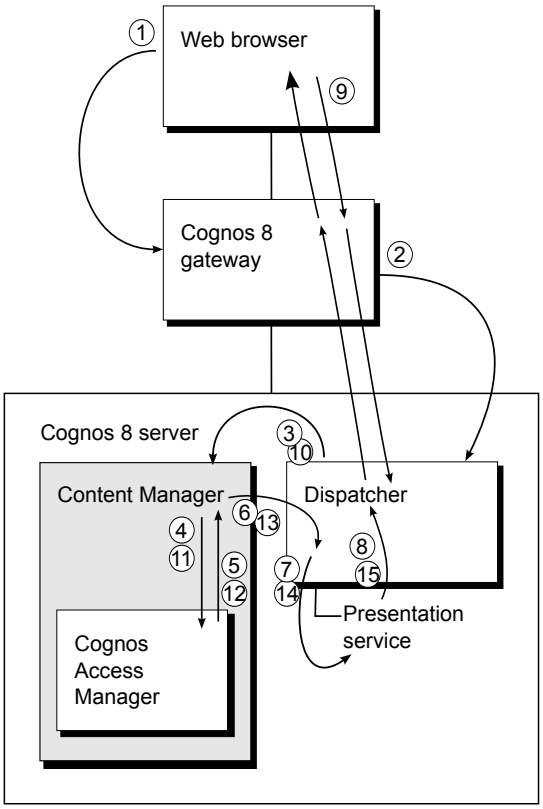


When a user requests anonymous access to Cognos 8, the following occurs:

1. The user attempts to access the Cognos 8 Welcome page or any other Cognos 8 user interface from a Web browser, sending a request to the Cognos 8 gateway.
2. The Cognos 8 gateway accepts the request and sends it to a dispatcher.
3. The dispatcher notes that there is no passport attached to the request, and sends the request to Content Manager.
4. Content Manager sends the request to Access Manager.
5. Anonymous access is enabled in this Cognos 8 system, so a passport is attached to the request and the request is returned through Content Manager to the dispatcher.
6. The dispatcher processes the request and sends it to the presentation service.

7. The presentation service sends the Welcome page back through the dispatcher and the gateway to the user.

Authenticated Access



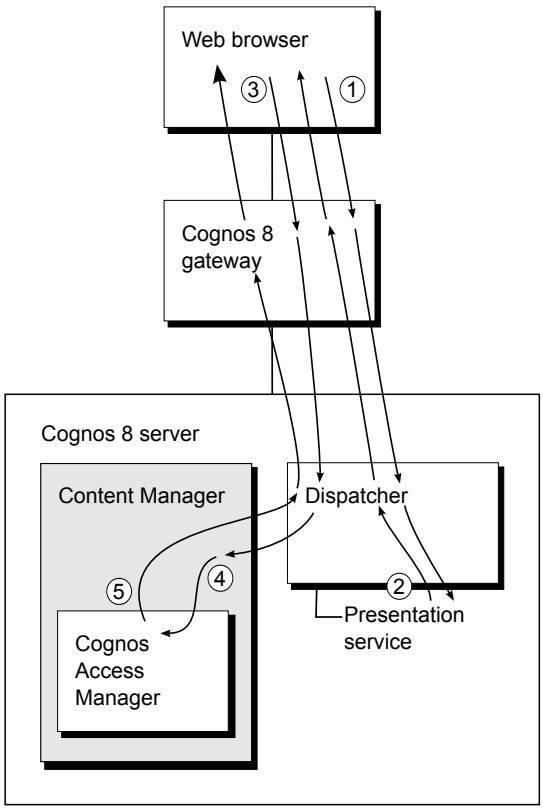
When a user requests authenticated access to Cognos 8, the following occurs:

1. The user attempts to access the Cognos 8 Welcome page or any other Cognos 8 user interface from a Web browser, sending a request to the Cognos 8 gateway.
2. The gateway accepts the request and sends it to a dispatcher.
3. The dispatcher notes that there is no passport attached to the request and sends the request to Content Manager.
4. Content Manager sends the request to Access Manager.
5. Anonymous access is disabled in this Cognos 8 system, so Access Manager sends the request back to Content Manager with a fault attached. The fault contains information about what is needed to log on. For example, if there are multiple namespaces, the user may be required to select a namespace. If there is only one namespace, the user may be required to provide a user ID and password.
6. Content Manager returns the request with the attached fault to the dispatcher.
7. The dispatcher sends the request to the presentation service.
8. The presentation service creates the appropriate logon page for the user, and returns the page through the dispatcher and the gateway to the user.
9. The user enters the required information, such as a user ID and password. The information is attached to the original request and sent through the gateway to the dispatcher.
10. The dispatcher sends the request to Content Manager.
11. Content Manager sends the request to Access Manager.
12. If all the required information is correct, Access Manager issues a passport, attaches it to the original request, and sends the request back to Content Manager. If the required information is incorrect or incomplete, then the request faults back to step 9.
13. Content Manager sends the request to a dispatcher.

14. The dispatcher processes the request and sends it to the presentation service.
15. The presentation service sends the Welcome page back through the dispatcher and the gateway to the user.

Viewing a Report or Analysis

Reports and analyses can be viewed in Cognos 8 in different formats, including HTML and PDF.



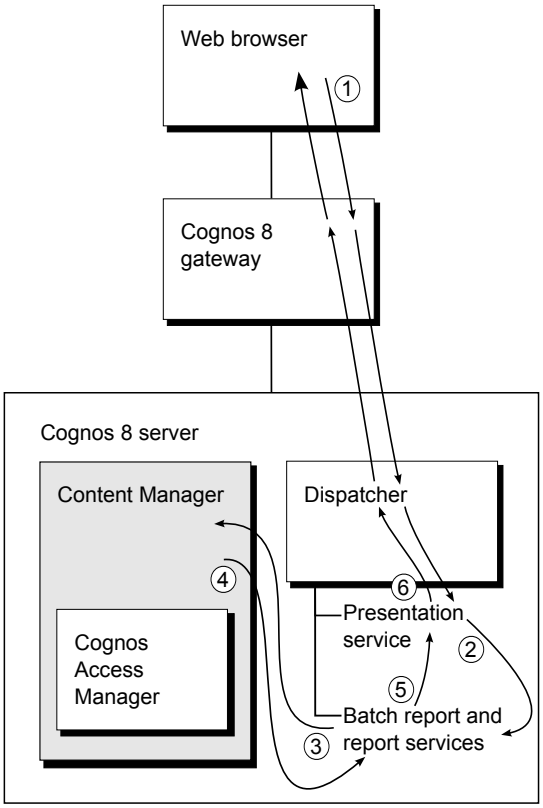
When an authenticated user views a saved HTML or PDF report or analysis through Cognos Connection, the following occurs:

1. The user clicks a report or analysis to view it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service returns the Cognos Viewer through the dispatcher and gateway to the browser. The Cognos Viewer has an HTML frame that shows the report or analysis page. The data view of the page contains a URL to a Content Manager object to be displayed.
3. The browser sends the URL through the gateway and dispatcher to Content Manager.
4. Content Manager checks with Access Manager to see whether the user has read privileges for the report or analysis. To do this, Content Manager sends Access Manager the access control lists for the report or analysis, the attempted action (read), and the user information.
5. Access Manager determines that the user can perform the action, and Content Manager sends the report or analysis in the form of an HTML page or PDF document through the dispatcher and gateway to the user. When serving a PDF report or analysis, byte serving is used.

Running a Report or Analysis

You can run a report or analysis in HTML or PDF format.

Running an HTML Report

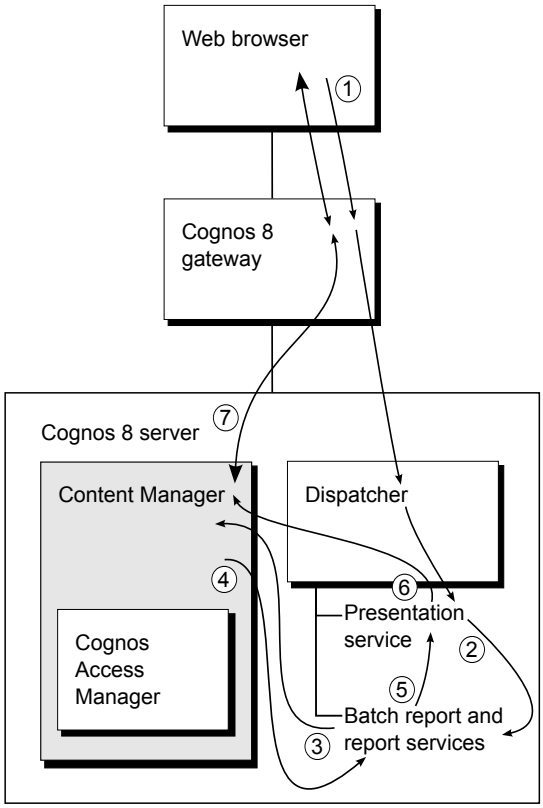


When a user runs an HTML report or analysis through Cognos Connection, the following occurs:

1. The user clicks a report or analysis to run it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to the report service through the dispatcher.
3. The report service requests the report or analysis and metadata from Content Manager, through the dispatcher.
4. Content Manager sends the report or analysis XML specifications and metadata to the report service. Content Manager refreshes metadata only when Cognos 8 is stopped and restarted or the model is updated and republished.
5. The report service returns one of these results to the presentation service:
   - an error page
   - a not ready page
   - a page of an HTML report or analysis
6. The presentation service sends one of these results through the dispatcher and gateway to the browser:
   - an error page
   - a wait or cancel page
   - a page of a completed HTML report or analysis in the Cognos Viewer interface

When the user presses page down or page bottom in the browser, the same path is followed again. The request has a high state of request affinity to ensure that it is routed to the same report service for additional rows of data. The report is cached so that the process does not have to restart.

Running a PDF Report or Analysis

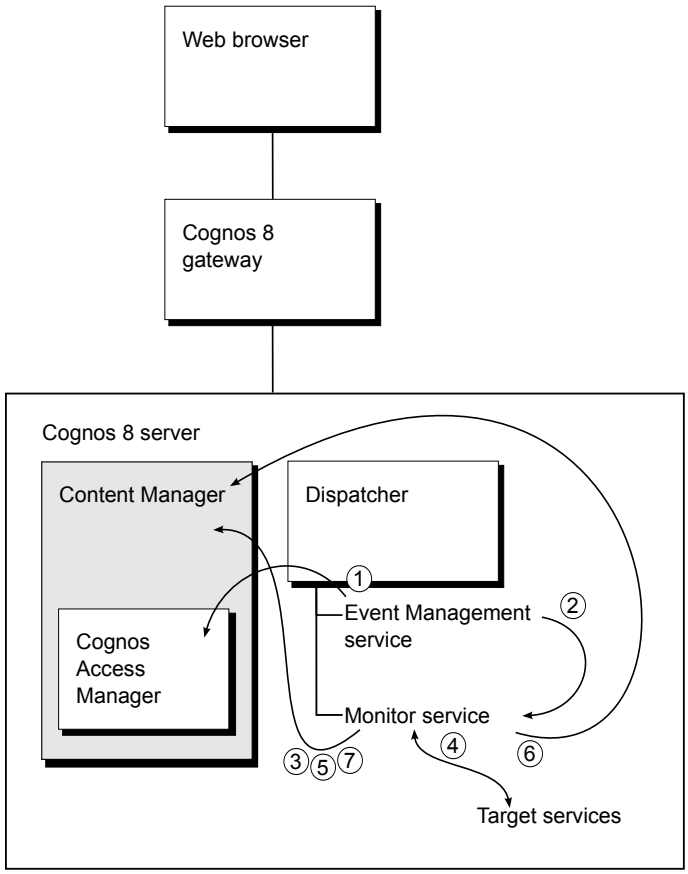


When a user runs a PDF report or analysis through Cognos Connection, the following occurs:

1. The user clicks a report or analysis to run it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to the report service through the dispatcher.
3. The report service requests the report XML specification and metadata from Content Manager, through the dispatcher.
4. Content Manager sends the report XML specification and metadata to the report service. Content Manager refreshes metadata only when Cognos 8 is stopped and restarted or the model is updated and republished.
5. The report service returns one of these results to the presentation service:
   - an error page
   - a not ready page
   - a PDF report or analysis
6. The presentation service sends the PDF result to Content Manager for storage in the user's session temporary area. Byte serving is used.
7. The wait/cancel page polls every few seconds to see if the report or analysis is complete. When it is complete, the Cognos Viewer HTML frame content is replaced with the PDF. A request is sent through the gateway and the dispatcher to the Content Manager and back with the PDF.

Scheduling a Task to Run

You can schedule a task to run for a report, query, analysis, data integration, agent, job, import, export, or content management.

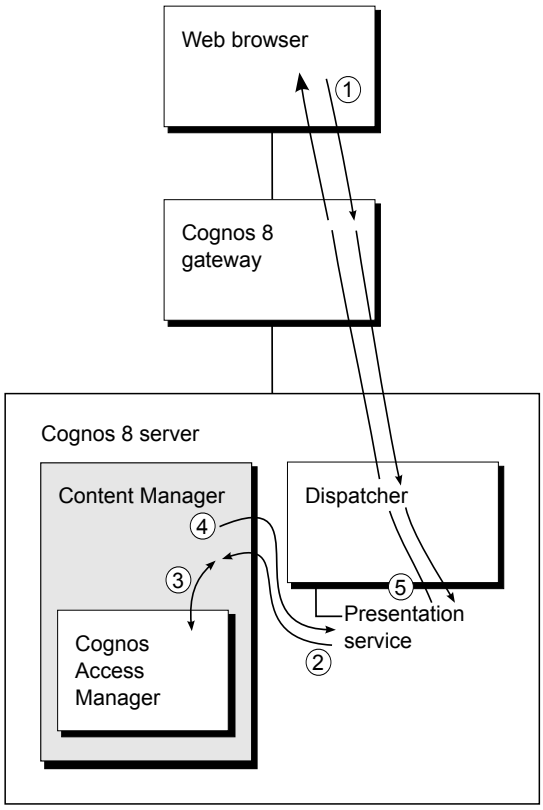


When a scheduled task runs, the following occurs:

1. At the scheduled time, the event management service sends a trusted request to Content Manager, via the dispatcher, to retrieve the user credentials, and then logs on as the user to obtain the user passport.
2. The event management service sends a request to the monitor service to run the scheduled task through the dispatcher. This request is a background request, and the conversation between the event management service and the monitor service ends.
3. The monitor service sends a request to Content Manager through the dispatcher to create a history object. This object is required to ensure that the correct status appears in the user interface.
4. The monitor service forwards the run request to the relevant service through the dispatcher and maintains the asynchronous protocol with the target service.
5. The monitor service updates the status of the history as "execution".
6. When the task completes, the target service stores any relevant information in Content Manager and ends communication with the monitor service. Information stored in Content Manager may include report output, agent event lists, and so on.
7. The monitor service detects the final state of the task run and updates the history object with a status that indicates whether the task was successful.

Opening a Cognos Connection Folder

Cognos Connection is a Web portal that comes with Cognos 8 (p. 14). You can also integrate Cognos 8 with your corporate Web portal.

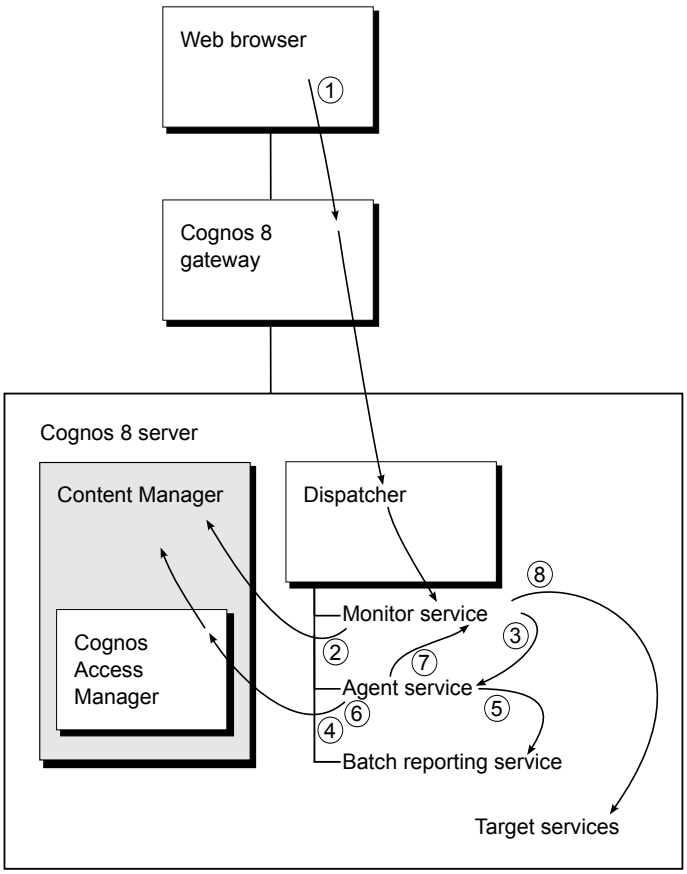


When a user opens a folder in Cognos Connection, the following occurs:

1. The user clicks a folder to open it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The presentation service sends the request to Content Manager through the dispatcher.
3. Content Manager checks with Access Manager to determine whether access is granted.
4. Content Manager sends the folder contents or an error message to the presentation service.
5. The presentation service formats the appropriate HTML page and sends it through the dispatcher and the gateway to the user.

Running an Agent

You can run agents to monitor your data and detect occurrences of business events.



When the user clicks an agent's run link, the following occurs:

1. The request goes through the gateway and the dispatcher to the monitor service.
2. The monitor service authenticates the request and creates a history in Content Manager for the agent run.
3. The monitor service forwards the request to the agent service. The monitor service maintains the asynchronous protocol (wait/cancel) on behalf of the gateway.
4. The agent service requests the agent definition and the previous agent event list from Content Manager.
5. The agent service executes the agent condition through the batch report service.
6. The agent service compares the generated result set with the previous event list, and creates and stores the updated agent event list in Content Manager.
7. Based on the authored agent tasks, the agent service executes its tasks through the monitor service.
8. The monitor service creates a history in Content Manager for each step and forwards the request (maintaining the asynchronous protocol) to the relevant service. For example, email messages are forwarded to the delivery service, reports are forwarded to the batch report service, and jobs are forwarded to the job service.

Portal Pages

Whether you are using Cognos Connection or a third-party portal, all Cognos functionality is available on the BI Bus. You can search for reports and view them in the portal and perform additional analysis, if needed. You can also monitor, configure, and administer Cognos users and content using the portal. Whether you are working with reports or performing administration tasks, requests are sent to the BI Bus and then forwarded to the appropriate Cognos 8 service for processing.

The following Cognos functions are commonly provided through portlets:

- Cognos Navigator retrieves selected Cognos 8 content.
- Cognos Search finds and opens published Cognos content.
- Cognos Viewer shows content selected in Cognos Navigator or Cognos Search.

For each portlet, all security permissions and credentials are inherited and passed along through the request. For example, if you go to a particular folder or search for a particular object, only those objects that you have permission to view are returned. Similarly, if you click a report in the Cognos Navigator or Search portlet, the report identifier and security credentials are included with the request. You can view the report in either the same portlet or a new portlet, but only the data that you have access to will appear.

Chapter 4: Workflow

The series of tasks that people in your organization will perform to understand, install, configure, and use Cognos 8 include the following:

- planning for implementation (p. 44)

  Implementation planning should be done before installing and configuring Cognos 8. It is typically carried out by a team assembled and led by the business intelligence solutions architect.

- installing and configuring (p. 44) Cognos 8

  Technical personnel install and configure Cognos 8, typically under the direction of the business intelligence solutions architect.

- administering Cognos 8 (p. 47)

  Administrators establish and maintain security, set up multilingual capabilities, install fonts, manage report distribution, and perform ongoing administration.

- working with models and packages to author reports and analyses for viewing (p. 47)

  Modelers create one or more metadata models, and use those models to publish packages that can be used to author reports and analyses (p. 48).

  Authors use published models to create and maintain reports and analyses (p. 49).

  Report users view and print reports and analyses through Cognos Connection. For more information, see the Cognos Connection *User Guide*.

  Authors and report users import report data to Microsoft Office workbooks and presentations using Cognos 8 Go! Office (p. 50).

- creating scorecarding applications and monitoring metrics (p. 50)

  Scorecard authors create packages that contain connection, report, and maintenance task information (p. 50). Authors then deploy, maintain, and access scorecard applications in Metric Studio (p. 51).

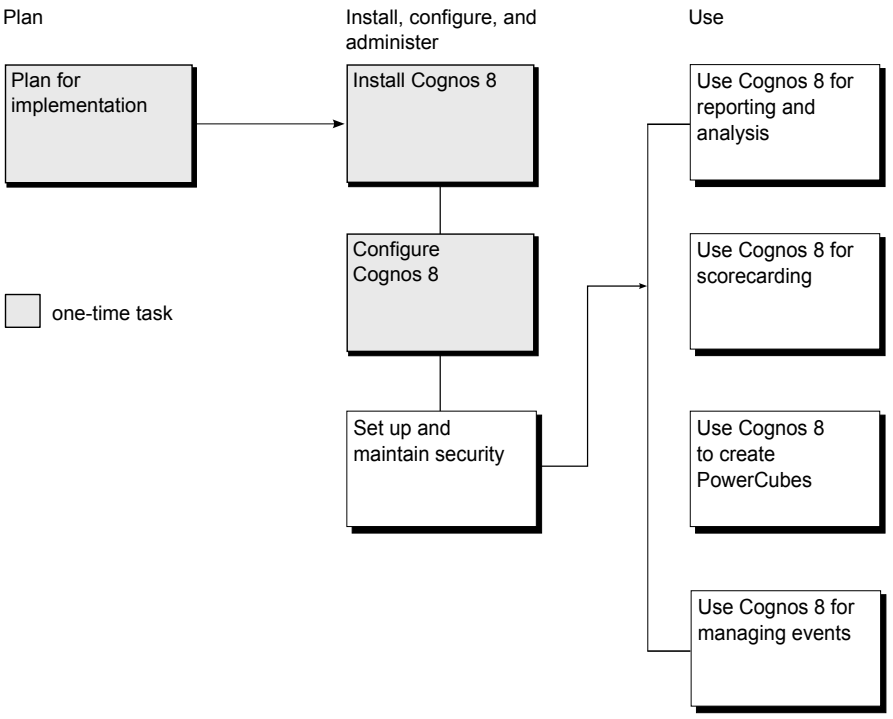
  Business users use metrics to monitor and analyze performance in key business areas. For more information, see the Metric Studio *User Guide for Authors*.

- creating Transformer models and PowerCubes (p. 51)

- Modelers create one or more metadata models and then use those models to create PowerCubes that can be used in reporting and analysis

- managing events (p. 52)

  Users create agents to monitor data and detect occurrences of business events.



Planning for Implementation

Implementing Cognos 8 means installing and configuring it to integrate effectively with your existing infrastructure.

To ensure that Cognos 8 is implemented effectively, it is important to plan your implementation carefully. For information about implementation planning, see the implementation planning checklist "Implementation Planning Checklist" (p. 53).

Installing Cognos 8

Installing Cognos 8 is typically done by Information Technology personnel under the direction of the business intelligence solutions architect.

When you install Cognos 8 using the **Installation** wizard, you specify where to install each of these components:

- gateways (p. 18)
- Application Tier Components (p. 19)
- Content Manager (p. 24)

You can install the components on one computer, or distribute them across a network. Before installing Cognos 8, choose the appropriate installation and configuration option (p. 55).

You must also install Framework Manager (p. 17), a Windows-based metadata modeling tool. The studio interfaces are HTML- and JavaScript-based, and do not require installation.

You can choose to install optional Windows-based metadata modeling tools. If you plan to use Cognos 8 for scorecarding, you can install Metric Designer (p. 17). If you plan to create PowerCubes in Cognos 8, you can install Cognos 8 Transformer (p. 17).

Unattended Installation

If you plan to install an identical Cognos 8 configuration across several computers on a network, or to install multiple configurations, you can set up and run an unattended installation. This is a noninteractive method of installing and configuring Cognos 8 in which all the tasks run automatically, without user intervention. You can run the unattended installation as part of a script, or from the command line.

An unattended installation is useful if you must install Cognos 8 at different geographic locations, some of which have no technical personnel to perform the installation.

For more information, see the *Installation and Configuration Guide*.

Configuring Cognos 8

One of the tools installed with Cognos 8 is Cognos Configuration. You use it immediately after installation to set the initial Cognos 8 configuration. Some of the things you can configure are

- logging

  You can specify the destination log for messages generated by Cognos 8 (p. 28).

- security

  You can run Cognos 8 with or without security. By default, the only security that is enabled is Cognos Application Firewall. If you want to set up security, you should configure security settings immediately after installing Cognos 8 (p. 107).

- data access

  You must specify database connection information for the Cognos 8 content store (p. 34).

Following initial configuration, if a property changes or components are added, you can use Cognos Configuration to reconfigure Cognos 8.

For information about initial configuration, see the *Installation and Configuration Guide*. For information about using Cognos Configuration, see the Cognos Configuration *User Guide*.

Monitoring Configuration Changes

Each time you save a configuration after making changes, date-stamped versions of these two configuration files are automatically saved in the *c8_location*/configuration directory:

- cogstartup.xml

  This file records configuration settings. An example is cogstartup_200211231540.xml

- coglocale.xml

This file records locale settings used for multilingual reporting. An example is coglocale_200211261401.xml

If you are unable to save a configuration, or you have problems with a configuration, you can revert to a previous configuration file. You can use the files to review your configuration history. Before calling Cognos Support for help, print a history of the configuration changes made in Cognos 8.

For more information about the cogstartup.xml and coglocale.xml files, see the *Installation and Configuration Guide*. For information about troubleshooting, see the Troubleshooting section of the *Administration and Security Guide*.

Configuring Security

Cognos 8 integrates with an existing security infrastructure to provide user authentication. Cognos 8 can secure content by using the user and group definitions from your security system, without any changes required. A Cognos namespace is included to provide the optional ability to define additional groups for securing content. These groups can simplify security administration by including users and groups from one or more authentication providers.

Cognos 8 includes Cognos Application Firewall, which is included with the dispatcher to validate and filter incoming and outgoing traffic at the dispatcher layer. By default, Cognos Application Firewall is enabled.

Cognos 8 also provides an authorization facility for assigning permissions to users defined in the authentication provider. It also provides a standard certificate authority (CA) for setting up encryption. Enhanced capabilities are available separately from Cognos.

If you intend to set up security for Cognos 8, it should be the first thing you do after installation (p. 107). For information about setting up and maintaining security, see the *Administration and Security Guide*.

Configuring Cognos 8 for Multilingual Reporting

Cognos 8 is a Unicode product capable of querying data in many languages and encodings. To facilitate multilingual reporting in Cognos 8, you may have to install additional fonts and configure your users' Web browsers.

Installing Fonts

Cognos 8 uses fonts to render PDF reports and to render charts used in PDF and HTML reports. To show output correctly, fonts must be available where the report or chart is rendered. This may involve installing additional fonts on the Cognos 8 server, and on the personal computers of Cognos 8 users. If users specify a font that is not installed, Cognos 8 substitutes a default font. For more information, see "Adding Fonts to the Cognos 8 Environment" (p. 99).

Configuring Browsers

Cognos 8 uses the default browser configurations of supported browsers. To ensure that Cognos 8 operates effectively, you should check your browser configuration settings and modify them if necessary. For information, see "Globalization Considerations" (p. 97).

Administering Cognos 8

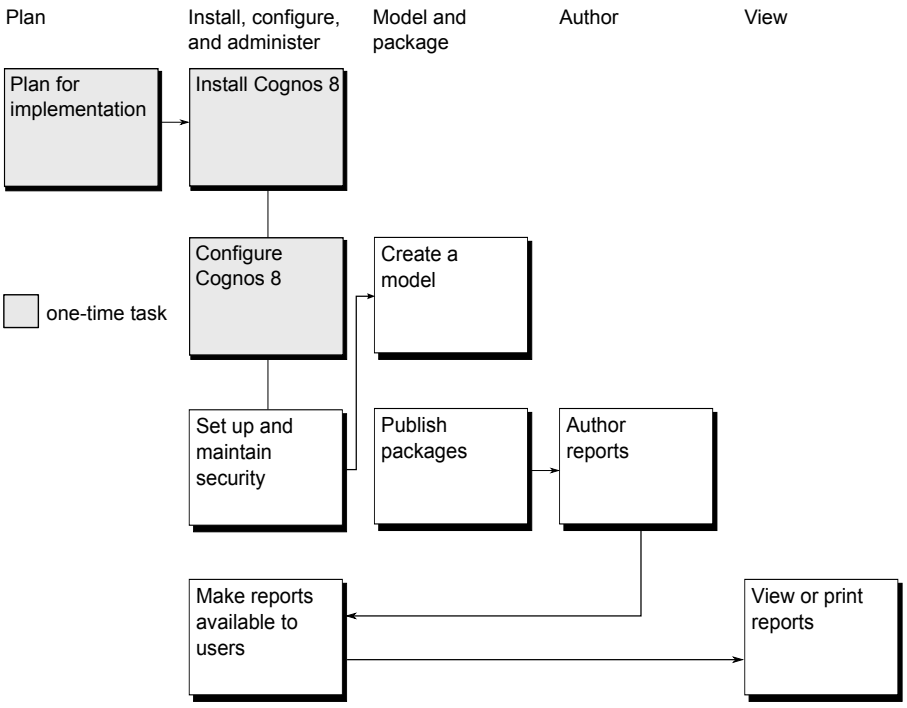
After Cognos 8 is installed and configured, you can use Cognos Connection (p. 14) or your third-party portal to

- define users, groups, and roles for security purposes
- set up folders where reports are stored
- make reports available to business users
- monitor and administer servers and activities
- back up data
- maintain security
- deploy Cognos 8 from one environment to another

For information about using Cognos Connection, see the Cognos Connection *User Guide*. For information about administration, setting up sample report projects and models, and troubleshooting problems, see the *Administration and Security Guide*.

Using Cognos 8 for Reporting and Analysis

The following diagram shows the complete reporting and analysis workflow for Cognos 8.



Creating Reporting Models and Packages

A model serves as an insulating layer between Cognos 8 reporting users and the database. Packages are model subsets that ensure users are provided with data appropriate for the reporting they need to do, and that the data is structured in ways that make sense from a business perspective.

Creating models and publishing packages are tasks that should be planned carefully. Models and packages that are well-designed from the start ensure that user requirements are met, data is secure, and your Cognos 8 application can be easily administered.

To understand the modeling and packaging process, users can study the sample models, packages, and reports provided with Cognos 8. For information about setting up the samples, see the *Administration and Security Guide*.

For Cognos 8 reporting, models and packages are created using Framework Manager. The following topics provide an overview. For more information, see the Framework Manager *User Guide*.

Modeling

Framework Manager is used to create a model that provides users with a single, integrated, business view of the database, and to provide Cognos 8 with information about how data is accessed, related, and secured.

A model that is designed to meet user requirements adds significant value to your data. It structures, adds to, and manages the data in ways that make sense to business users. Creating a model is an important task that should be planned and executed by a modeler or a modeling team familiar with both the database structure and the needs of your business users.

When you create a model, you

- specify the metadata to import from data sources defined in the Cognos 8 content store
- refine the metadata by adding business names, descriptions, multilingual values, calculations, filters, and other components
- specify joins and relationships
- organize the data for presentation in ways that make sense to business users and add value to your databases
- add security to the metadata to determine who can use the metadata and for what purposes

Packaging

After a model is created, packages are published to locations on the Cognos 8 server where report authors can use them to create reports. A different package, containing only the necessary information, can be published for each group of users.

Reports cannot contain data from more than one package. When publishing a package, it is important to ensure that the package contains all the data required to meet the needs of the intended users.

The hierarchical structure of a package controls the way in which folders, reports, and other data objects are structured in the interface used by the report author. It also controls how security is applied to the objects, and how easy it is to deploy the package to other environments. As a result,

it is important to ensure that the structure of a package makes sense from the perspective of a business user, and not just from an administrative perspective.

Authoring Reports

Cognos 8 can be used to create many different types of reports, including lists, crosstab reports, charts, master and detail reports, and user-designed reports. You create planned, professional reports in Report Studio, and ad hoc reports in Query Studio. You can explore and analyze data in Analysis Studio. You can use report data from Report Studio, Query Studio, and Analysis Studio in Microsoft Office applications through Cognos 8 Go! Office.

The Cognos 8 architecture is fully open to third-party products and to custom development. Cognos 8 can be integrated with existing transaction-based Web products or portals. For information about custom development, see the Cognos 8 SDK *Developer Guide*. For information about integrating Cognos 8 with other enterprise portals, see the *Administration and Security Guide*.

Query Studio

Report authors and users create ad hoc reports using Query Studio. Ad hoc reports, also called ad hoc queries, can be created quickly, with little or no training, to meet reporting needs not covered by standard, professional reports.

Authors can save query specifications for future revision, or as templates for other new reports. Reports can be made available in interactive mode, so that users can expand them, or in read-only mode. Reports created in Query Studio can be viewed and edited in Report Studio.

Before creating ad hoc queries, users should complete the tutorial provided to familiarize themselves with best practices in report creation. For more information, see the *Getting Started Guide*.

For information about Query Studio, see the Query Studio *User Guide*.

Report Studio

Report authors create professional reports using Report Studio. Planned reports are standard, professional reports designed to meet specific, recurring needs of business users. Authors can also use Report Studio to edit reports generated in Query Studio.

To create a report in Report Studio, an author specifies the model that will provide data for the report. The author then builds a report specification that defines the queries and prompts used to retrieve the data. The author also creates the layouts and styles used to present the data. In addition to creating new reports, authors can modify existing reports.

Before creating reports for corporate use, report authors should use the tutorial provided to familiarize themselves with best practices in report creation. For more information, see the *Getting Started Guide*.

For information about Report Studio, see the Report Studio *User Guide*.

Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled

relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

Before creating an analysis, the administrator must have created a package in Framework Manager and published it to a location in the Cognos Connection portal for user access. Users can then select the package and find the data they require for the analysis. Users may also choose to share findings with others.

For information about using Analysis Studio, see the Analysis Studio *User Guide* or the online Quick Tour.

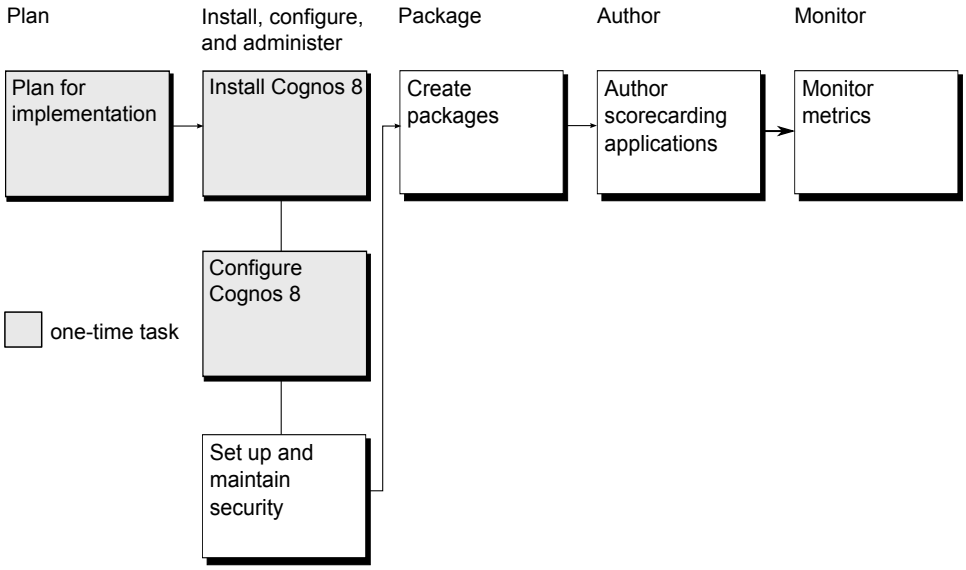
Cognos 8 Go! Office

Authors and report users may want to use data from Cognos reports in Microsoft Office workbooks, documents, and presentations. In Cognos 8 Go! Office, users can import or remove Cognos report elements from Microsoft Excel workbooks, Microsoft Word documents, and Microsoft PowerPoint presentations. Users can run reports using the Cognos studios and publish workbooks and presentations to Cognos Connection.

For information about using Cognos 8 Go! Office, see the Cognos 8 Go! Office *User Guide*. For more information about configuring and deploying Cognos 8 Go! Office, see the *Installation and Configuration Guide*.

Using Cognos 8 for Scorecarding

The following diagram shows the complete scorecarding workflow for Cognos 8.



Packaging in Metric Studio

A metric package is a Cognos Connection representation of a Metric Studio scorecarding application. A metric package contains connection information, reports, and metric management tasks for that application. The metric package content is stored in a metric store.

You must create a package the first time you access Metric Studio. You can create other packages in Cognos Connection or Metric Studio. For more information, see the Metric Studio *User Guide for Authors*.

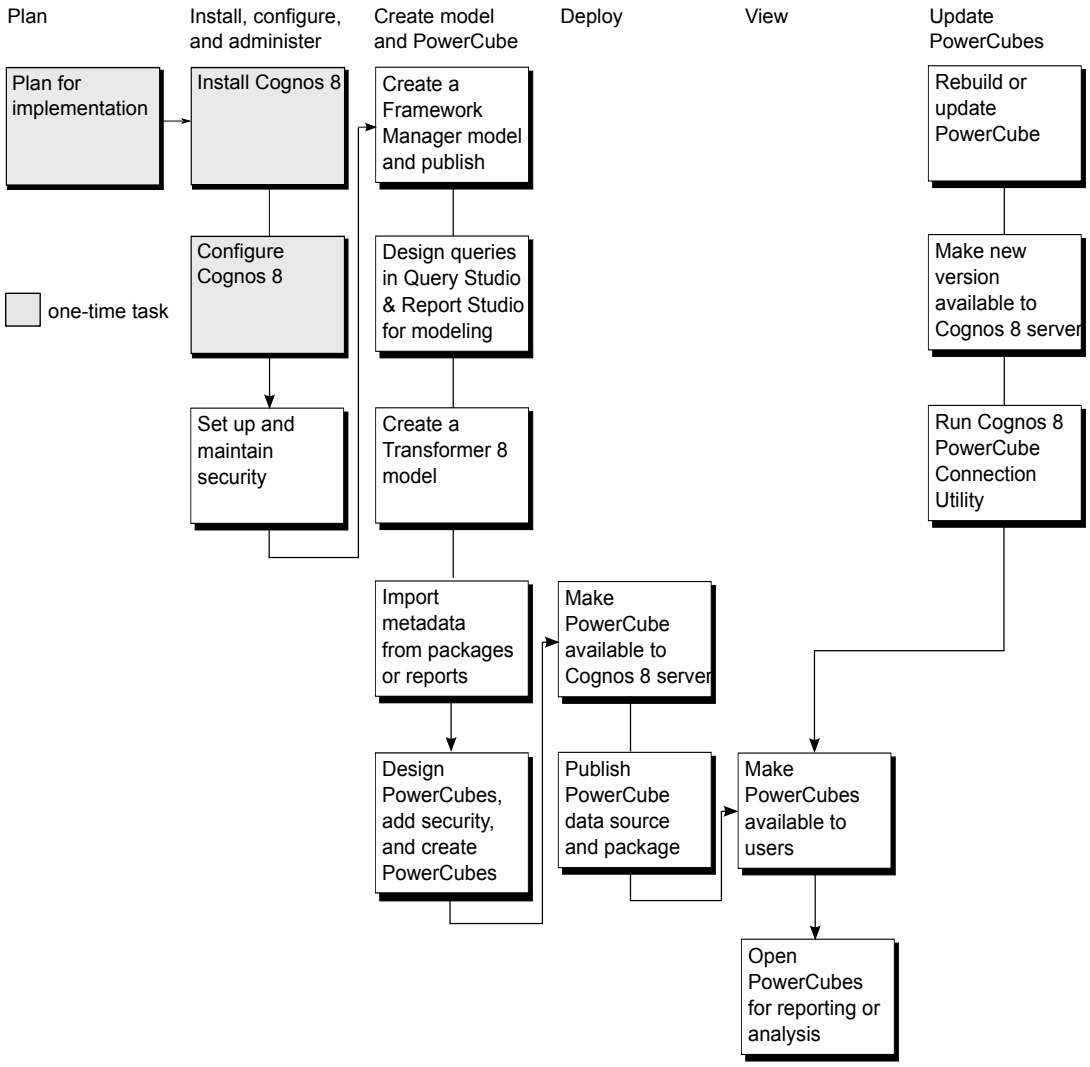
Authoring Scorecarding Applications

A scorecarding application is a set of scorecards, metrics and projects used to monitor the performance of a specific aspect of an organization.

You create scorecarding applications using Metric Studio. You use a Metric Studio package to deploy, maintain and access a scorecarding application. For more information, see the Metric Studio *User Guide for Authors*.

Using Cognos 8 to Create PowerCubes

The following diagram shows the complete Transformer model and PowerCube workflow for Cognos 8.


Plan
Install, configure, and administer
Create model and PowerCube
Deploy
View
Update PowerCubes
Plan for implementation
Install Cognos 8
Create a Framework Manager model and publish
Rebuild or update PowerCube
Configure Cognos 8
Design queries in Query Studio & Report Studio for modeling
Make new version available to Cognos 8 server
one-time task
Set up and maintain security
Create a Transformer 8 model
Run Cognos 8 PowerCube Connection Utility
Import metadata from packages or reports
Make PowerCube available to Cognos 8 server
Design PowerCubes, add security, and create PowerCubes
Publish PowerCube data source and package
Make PowerCubes available to users
Open PowerCubes for reporting or analysis

Managing Events

An event is any situation that can affect the success of your business. To ensure that the appropriate personnel are made aware of an event, you create agents in Event Studio to monitor your data and detect occurrences of business events.

Chapter 5: Implementation Planning Checklist

To get the most from Cognos 8, you must implement it effectively. This means installing and configuring Cognos 8 so that it integrates with your information technology infrastructure and meets your reporting requirements.

To plan an effective Cognos 8 implementation, do the following:

- Familiarize yourself with the Cognos 8 architecture.

  Read Part 1 of this book. It will help you understand the components that make up Cognos 8, their functions, and the ways in which they interact with each other, your infrastructure, and your authors and users.

- Decide how to install and configure Cognos 8 (p. 55).

  Know what your options are for installing and configuring Cognos 8, and decide which best meet your needs.

- Decide how to maximize Cognos 8 performance in your environment (p. 69).

  Understand the factors that can affect Cognos 8 performance, and plan to ensure and maintain adequate capacity, scalability, and availability for Cognos 8 in your environment.

- Decide how to configure Cognos 8 multilingual capabilities (p. 97).

  If you will use Cognos 8 in a global environment, decide how to configure Cognos 8 so that interface elements and report contents appear in the languages that users need.

When you complete your planning and are ready to install and use Cognos 8, refer to the other Cognos 8 documents for step-by-step instructions (p. 7).

Chapter 6: Installation Options

Before implementing Cognos 8, decide how you will install and configure it to provide the best possible performance. The installation and configuration choices that produce the best performance depend on your reporting requirements, resources, and preferences.

When you assess your installation options for Cognos 8, you must consider whether you are installing the product for the first time or upgrading. For information about upgrading, see the *Installation and Configuration Guide*.

When you install Cognos 8, you specify where to install the gateways, Application Tier Components, and Content Manager. You can install all Cognos 8 components on one computer, or distribute them across a network.

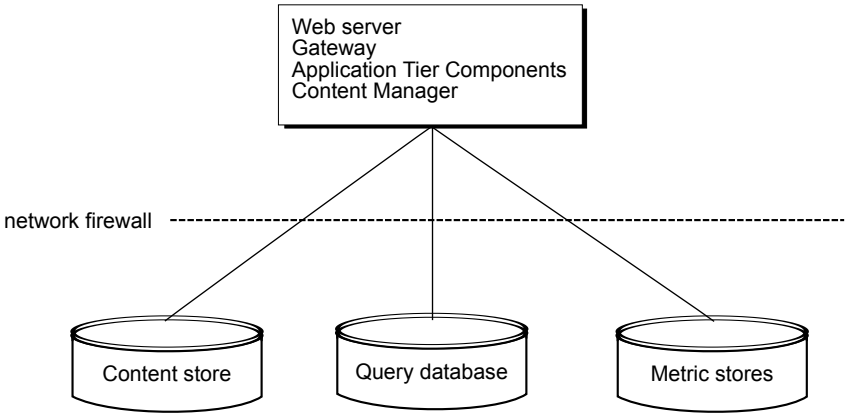
You must install Framework Manager, the metadata modeling application for business intelligence. You can choose to install optional metadata modeling applications such as Metric Designer for scorecarding and Transformer for creating PowerCubes.

Cognos 8 is compatible with other Cognos products. If your environment includes other Cognos products, you must consider how Cognos 8 will fit into that environment. For more information, see "Cognos 8 with Other Cognos Products" (p. 63).

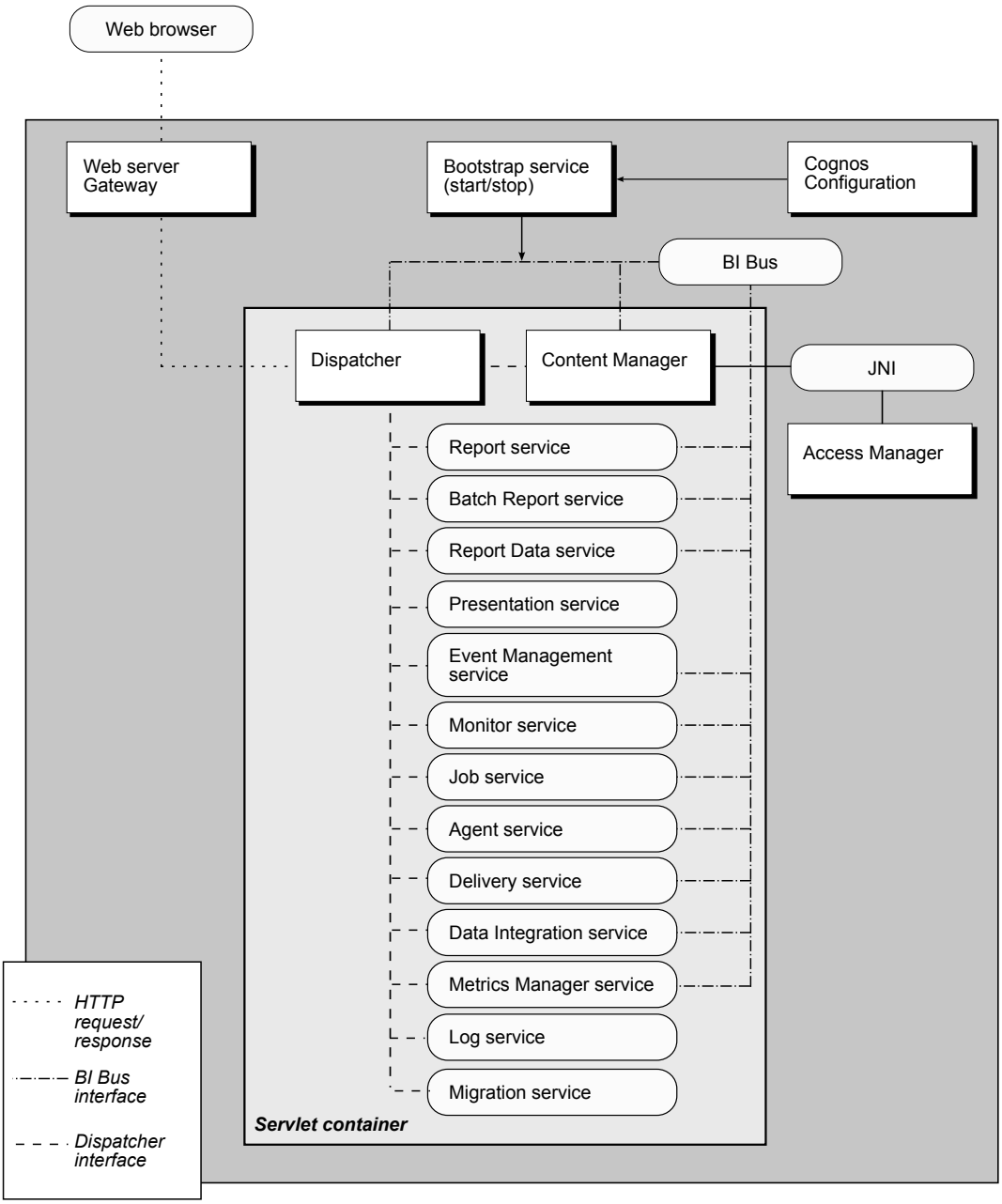
Installing All Components on One Computer

Install all components on one computer only for proof of concept or in demonstration environments where the user load is small. Because the gateway must be located with the Web server, the single computer must also be running a Web server.

In the following diagram, all Cognos 8 components are installed on one computer.



The following diagram provides a more detailed view of a Cognos 8 installation in which all server components are installed on a single computer. The modeling components, such as Framework Manager, Metric Designer, and Transformer, can be installed on different computers.



If Cognos 8 is installed on a Windows platform, you can install the modeling tools on the same computer. If Cognos 8 is installed on a UNIX or Linux platform, you must install the Windows-based modeling tools on a separate computer that runs under Windows.

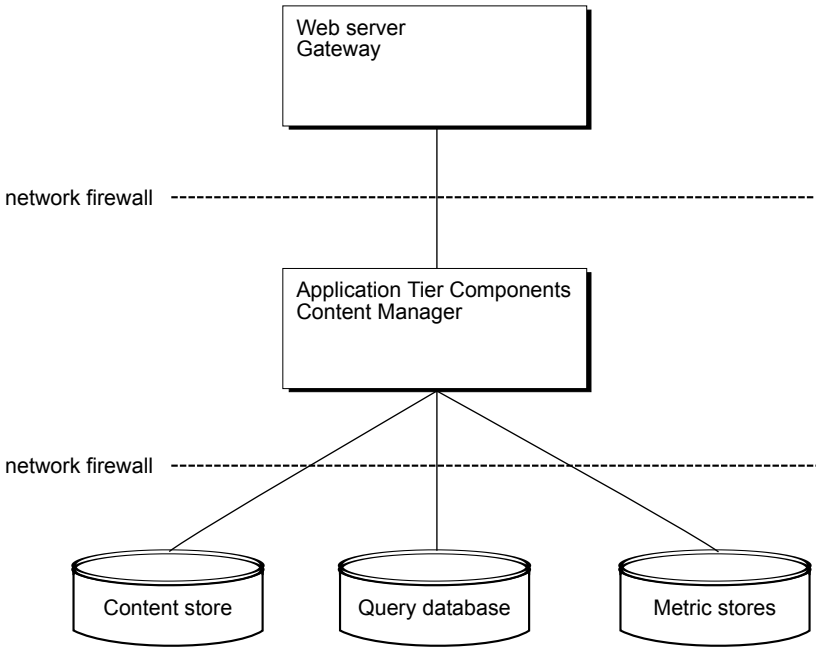
Installing the Gateway on a Separate Computer

You can install the gateway and a Web server on one computer, and install the remaining Cognos 8 components on other computers. If you have a Web farm, you may want to install a Cognos 8 gateway on each Web server. Using multiple Web servers to manage incoming requests provides a better level of service.

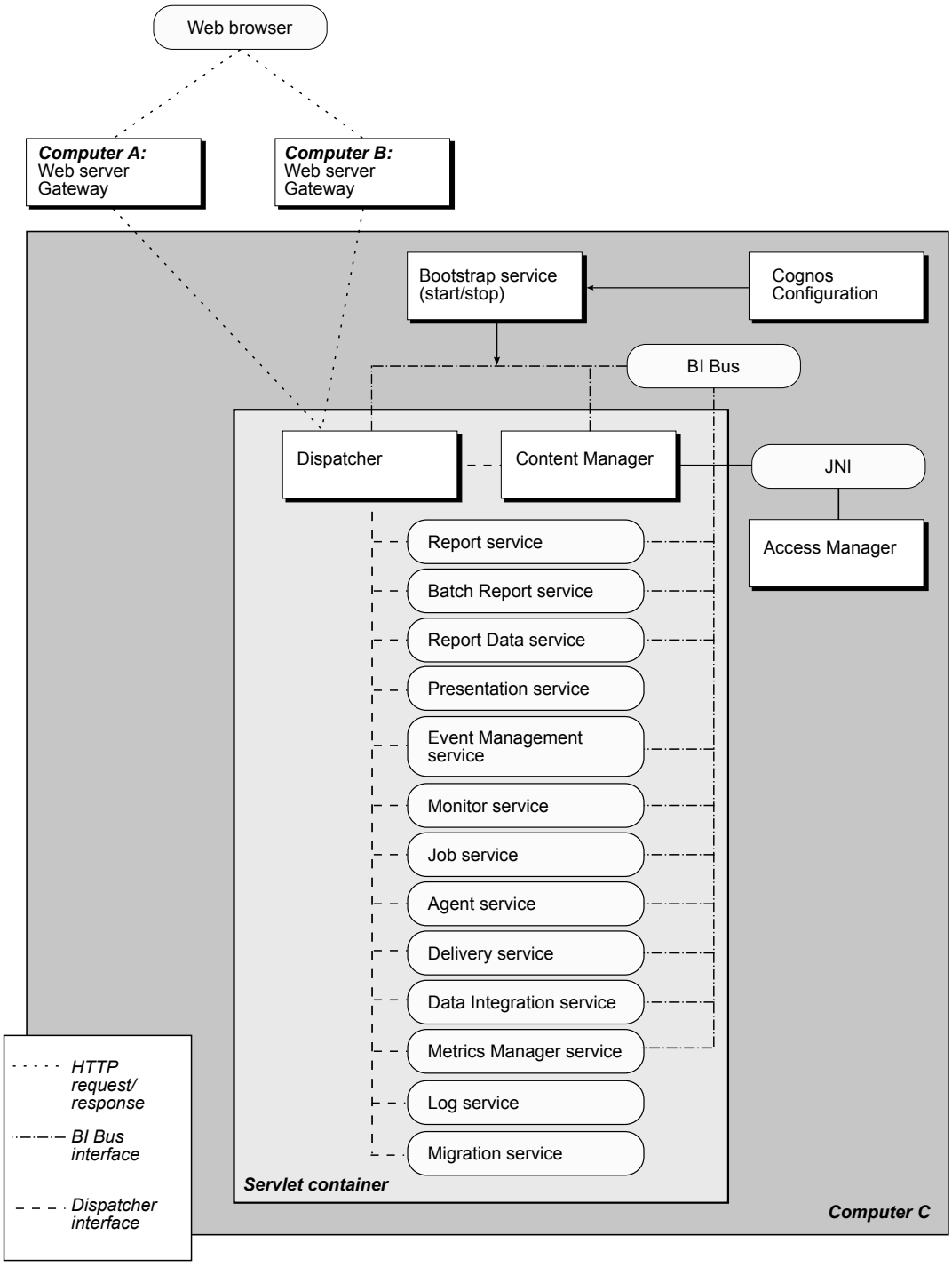
If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of

processing may be required if you have a network firewall between the Web server and your Application Tier Components computers.

In the following diagram, the Web server has a gateway installed. Incoming requests are passed to the gateway and forwarded to the Application Tier Components computer. If request information is not saved, the result is returned from the Application Tier Components computer. If request information is saved, it is saved in the content store.



The following diagram provides a more detailed view of an installation in which the gateway is on a separate computer from other Cognos 8 components. In this example, two Web servers are used, each with a gateway.



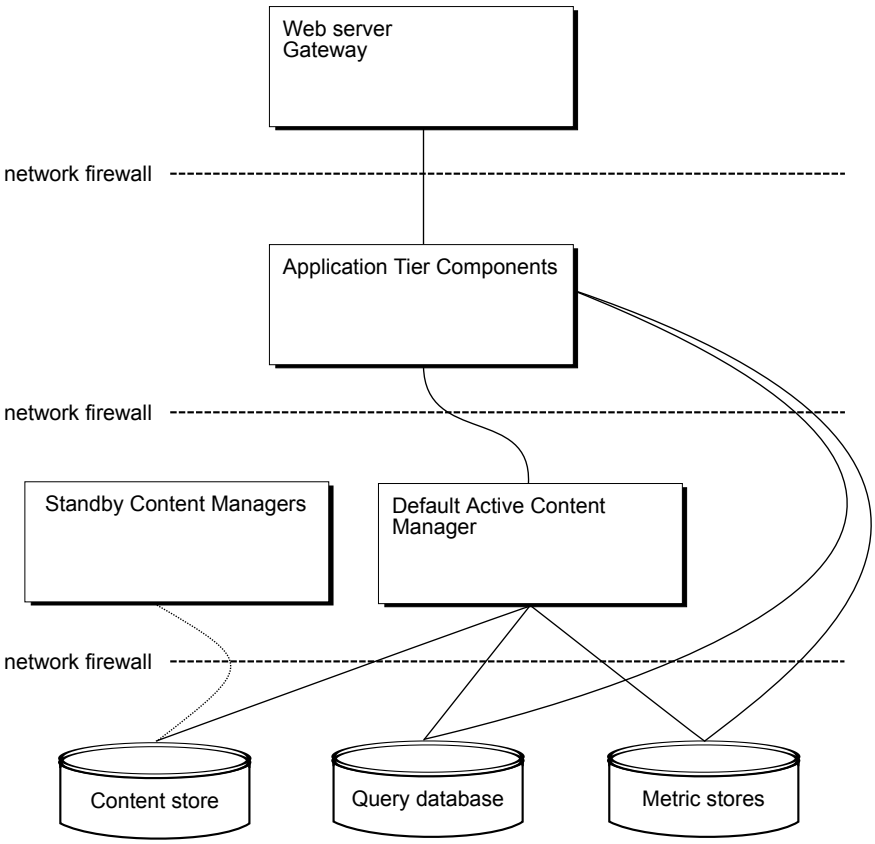
Installing Application Tier Components and Content Manager on Separate Computers

Installing Application Tier Components on separate computers from the Content Manager can improve performance, availability, and capacity.

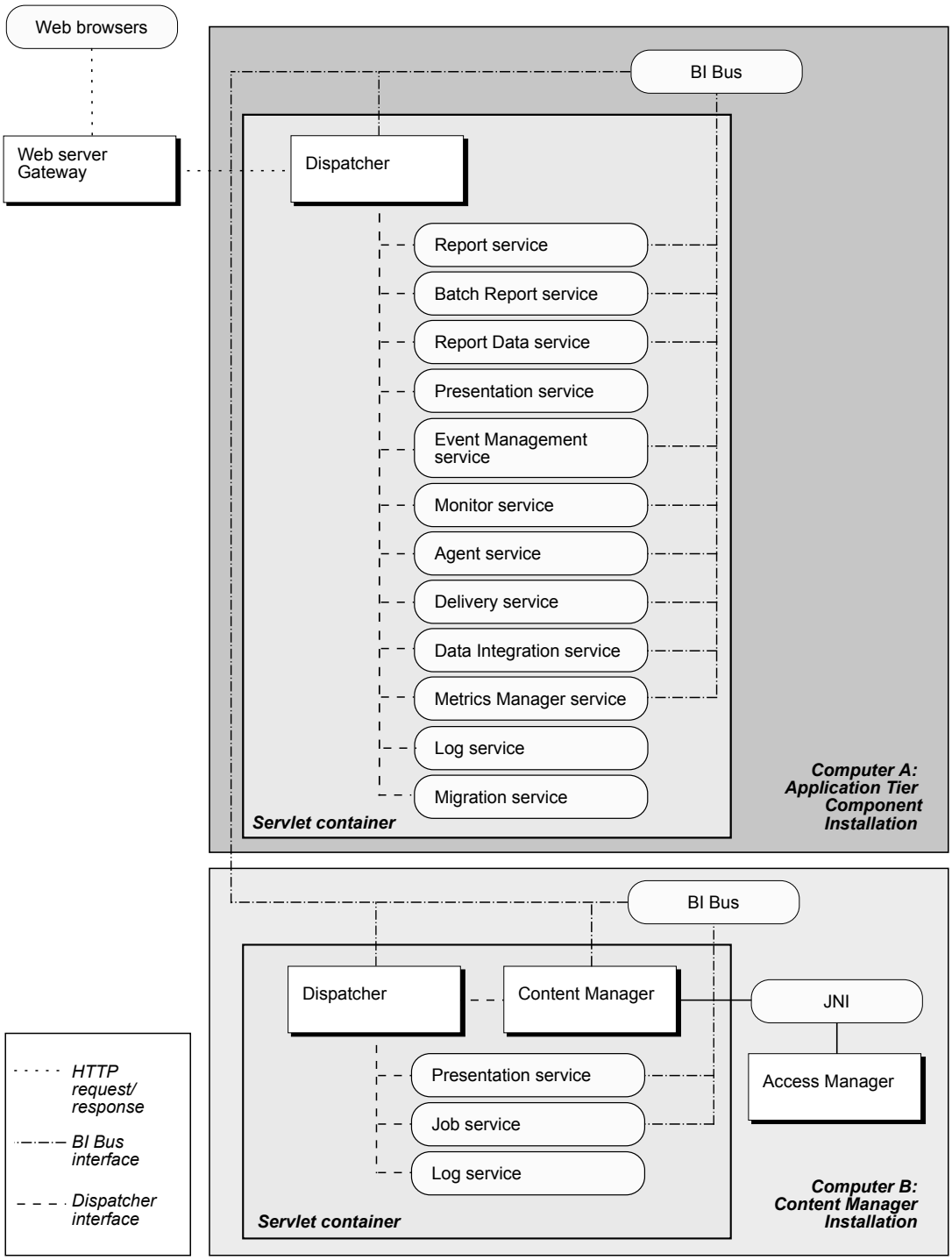
You may choose to install Content Manager separately from the Application Tier Components to isolate and protect sensitive data that is managed by Content Manager.

You may also choose to install Content Manager on a separate computer if large volumes of data are managed by Content Manager. In this type of environment, Cognos 8 scalability can be improved by increasing the size of the processor on which Content Manager is installed.

In the following diagram, incoming requests are routed to a gateway. The gateway forwards the request to the Application Tier Components computer. The Application Tier Components computer forwards it to the active Content Manager computer, which queries the content store and sends the results back to the Application Tier Components computer for rendering.



The following diagram shows a more detailed view of a Cognos 8 installation in which separate computers are used for Application Tier Components and the Content Manager. This example shows only one installation of Application Tier Components, however the Cognos 8 environment can include multiple Application Tier Components computers.



Multiple Installations of Content Manager

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby. The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

Multiple Application Tier Components

To improve scalability in an environment in which there is typically a large volume of report requests to process, you can install Application Tier Components on multiple computers dedicated to processing incoming requests. By installing Application Tier Components on multiple computers, you distribute and balance loads among the computers. You also have better accessibility and throughput than on a single computer, as well as failover support.

Modeling Tool Installation Options

The Cognos 8 modeling tools, Framework Manager, Metric Designer, and Transformer, can be installed either on a computer containing other Cognos 8 components, or on a computer that is separate from these other components.

The modeling tools communicate with the Application Tier Components, which can be installed on one or more Web servers. Modeling tools can communicate with Application Tier Components using one of these routes:

- connect to the Application Tier Components dispatcher using the Internal dispatcher URI. This route is the recommended route.
- connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the Internal dispatcher URI. You must configure appropriate security for this gateway. This method is useful when the modeling tool is outside a network firewall.

  Important: Do not change your main gateway to use the Internal dispatcher URI. Doing so reduces the security of the Cognos 8 portal and studios.

To publish Framework Manager models, Metric Designer extracts, or Cognos 8 Transformer PowerCubes, you must configure the modeling tool to communicate with a dispatcher, either directly or through a dedicated gateway.

To ensure that the modeling tool can communicate with Cognos 8 components, on the computer where the tool is installed, configure cryptographic properties and the following environment properties:

- Gateway URI
- Dispatcher URI for external applications

For more information, see the *Installation and Configuration Guide*.

Web Servers Other Than Microsoft IIS

For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the two communication routes between the modeling tool and the Application Tier Components dispatcher. For either route, the modeling tool uses the BI Bus SOAP API. If you use

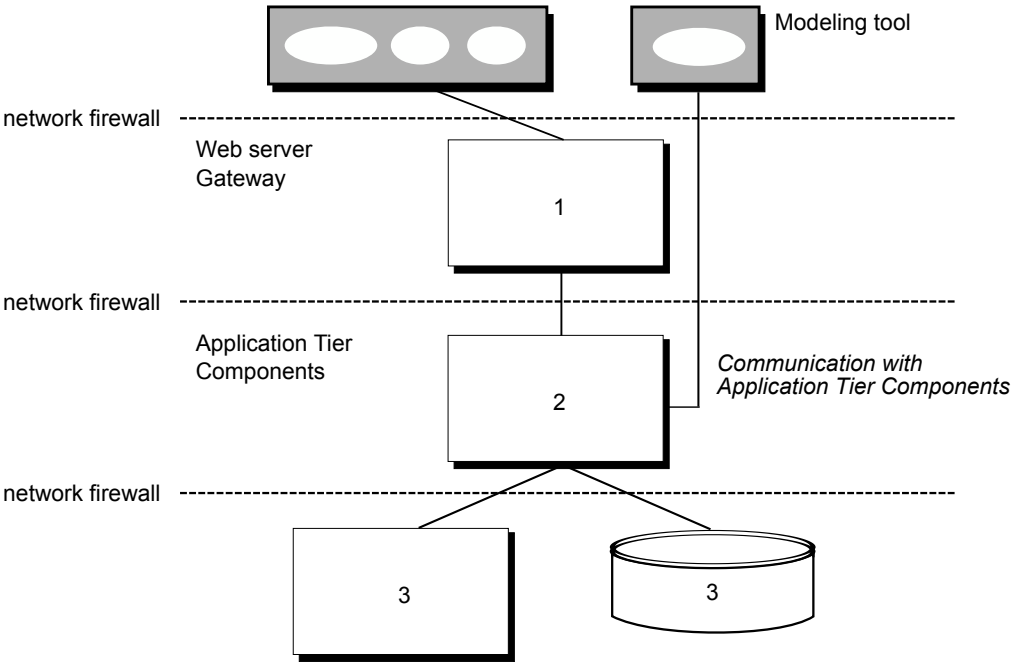
the Web server route, and you have medium-sized and large models (approaching 1 MB in size), the models are broken into smaller pieces (chunked) for transmission.

If you use a Web server other than Microsoft IIS, we recommend that you configure the modeling tool to communicate through your Web server gateway (Route 1). This eliminates the need to set up additional communications channels if you use firewalls to separate the modeling tool, your Web server, and your Application Tier Components.

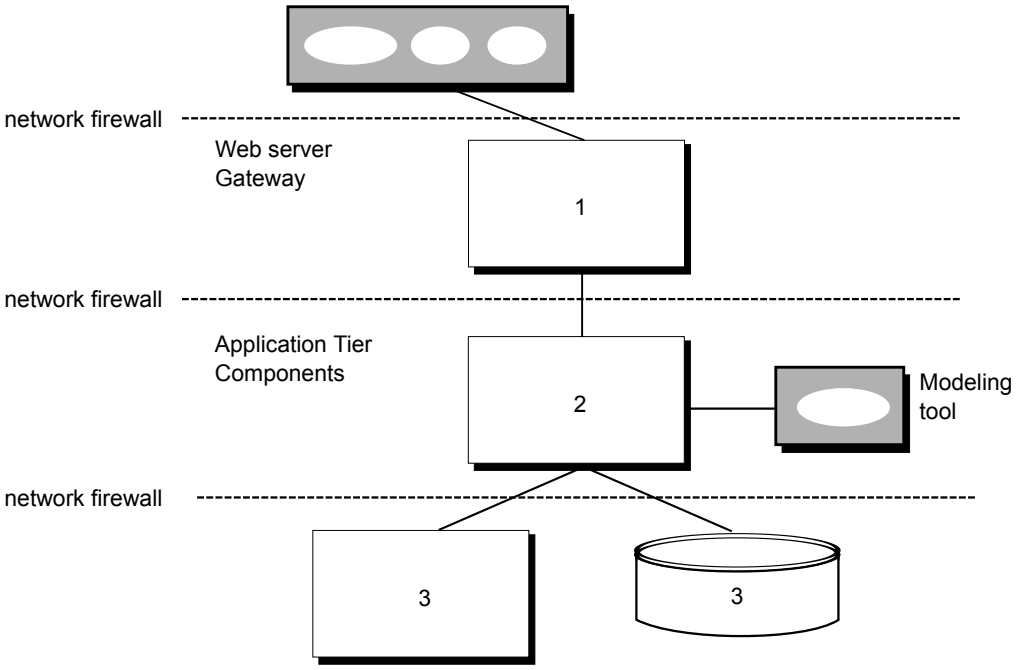
Network Firewall Considerations

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default Cognos 8 configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

By default, the modeling tool is configured to send requests directly to the dispatcher:



To avoid communication issues when communicating directly with the dispatcher, install the modeling tool in the same architectural tier as the Application Tier Components.



Alternatively, you can install an additional gateway that is dedicated for communication with the modeling tool. You then configure the modeling tool and its gateway such that the dispatcher will accept requests from the modeling tool. In addition to the environment properties that must be configured for the modeling tool, you must configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

Cognos 8 with Other Cognos Products

You can install Cognos 8 in an environment that includes other Cognos products. The installation wizard for Cognos 8 can recognize compatible directories and shows a warning when conflicts occur. After Cognos 8 is installed, you can access objects that are created in another Cognos product in Cognos 8. The requirements for access depend on how you choose to run the two products.

Cognos Products That Can Be Upgraded to Cognos 8

The following Cognos products are earlier versions of components that are now within Cognos 8: ReportNet, Cognos Metrics Manager, DecisionStream, and PowerPlay Web. When you upgrade these products to Cognos 8, you can continue to run the earlier versions concurrently in the same environment until you are satisfied with the transition to Cognos 8.

ReportNet®

For ReportNet and Cognos 8 to run concurrently, each version must have unique ports, content stores, aliases, and cookie settings. If you use the default settings, configuration is required only to select new ports and a new content store for Cognos 8. You cannot use data from ReportNet directly in Cognos 8 until you upgrade ReportNet. When you upgrade to Cognos 8, the content store is upgraded to use the Cognos 8 schema. You can upgrade reports at the same time or upgrade them later if compatibility is required with some existing SDK applications.

For instructions about running concurrently and upgrading, see the upgrade chapter in the *Installation and Configuration Guide*.

Cognos Metrics Manager

To use data store content from Cognos Metrics Manager in Cognos 8, you upgrade by exporting the content from the data store, installing Cognos 8, and then importing the content into the Cognos 8 metric store. Note that the cube picker feature (the ability to map specific metrics to cube intersections) in Cognos Metrics Manager is not available in Cognos 8.

For instructions about upgrading, see the upgrade chapter in the *Installation and Configuration Guide*.

Cognos DecisionStream

You can continue to run Cognos DecisionStream Series 7 concurrently with Cognos 8 products. Catalogs that are created using DecisionStream Series 7 must be upgraded before you can use them with Data Manager.

For instructions about running concurrently and upgrading DecisionStream catalogs to the Cognos 8 Data Manager environment, see the chapter about upgrading a catalog in the Data Manager *User Guide*.

Cognos PowerPlay Web

You can continue to use PowerPlay Web reports within the PowerPlay 7 user interfaces in the Cognos 8 portal. You can also drill through between PowerPlay Web and Cognos 8. You can publish from PowerPlay Enterprise Server to Cognos 8, provided that you use the same host name or IP address to identify the Series 7 namespace in Cognos Series 7 and in Cognos 8.

You can also upgrade the following reports to Cognos 8 reports by using migration tools:

- PowerPlay Windows reports
- PowerPlay Web Explorer reports
- PowerPlay for Excel reports
- PowerPlay for Windows reports published to PowerPlay Web

The tools are available at the Cognos Global Customer Services Web site (support.cognos.com).

For instructions about upgrading, see the Migration Tools *User Guide*.

Cognos Series 7 Products That Can Be Migrated to Cognos 8

You can migrate metadata and applications from Cognos Series 7 to Cognos 8. Content that can be migrated includes Architect models from Windows, Impromptu client reports and catalogs from Windows, Upfront content, and Web-based content from Windows and UNIX.

For more information, see the Migration Tools *User Guide*.

For a list of supported Cognos Series 7 versions and to download the migration tools and documentation, see the Cognos Global Customer Services Web site (http://support.cognos.com).

Architect

You can migrate Architect models for use as a metadata source for Framework Manager.

Impromptu

You can migrate Impromptu catalogs and reports to Cognos 8. You use migrated catalogs as a metadata source for Framework Manager. After completing the catalog migration process, you can migrate and deploy Impromptu reports.

Upfront

You can migrate Upfront content to Cognos 8. The migration process maps the Upfront content structure to a Cognos Connection folder structure. By preserving the existing Upfront organization, it is easier to complete administrative tasks, such as applying security to the migrated content.

Impromptu Web Reports

You can migrate Impromptu Web Reports content, such as schedules and events, to Cognos 8. You migrate Impromptu Web Reports content using a Cognos Series 7 Deployment Manager package as the migration source. Before you migrate Impromptu Web Reports you must migrate the Impromptu catalog metadata used by the reports.

You cannot migrate Impromptu query definition files (.iqd), but you can continue to use existing .iqd files to build cubes in Cognos 8 BI Transformer 8.3. To do so, you must install the optional component, Series 7 IQD Bridge, which is available to install with Cognos 8 BI on Cognos Series 7 supported platforms.

PowerPrompts are not migrated, but you can implement similar functionality using either the built-in administrator functionality or the Software Development Kit.

Cognos Products That Interoperate with Cognos 8

Some Cognos products provide functionality that is not available in Cognos 8. You can use these products in the same environment as Cognos 8. With some products, you can access the different types of cubes or reports in the Cognos 8 portal. With other products, you can access unique features in the Cognos 8 portal.

Cognos Planning - Analyst

You can access published plan data in Cognos 8 by using the Generate Framework Manager Model wizard, which requires Cognos Planning - Analyst 7.3 MR1 or later.

For more information, see the Analyst *User Guide*.

Cognos Planning - Contributor

You can access unpublished (real-time) Contributor cubes in Cognos 8 by custom installing the Cognos 8 - Contributor Data Server component that is included with Cognos Planning - Contributor 7.3 MR1 release or later. You can access published plan data in Cognos 8 by using the Generate

Framework Manager Model administration extension in Contributor, which requires Cognos Planning - Contributor 7.3 MR1 or later.

For more information, see the Contributor *Administration Guide*.

Cognos Finance

You can access Cognos Finance cubes that are secured against a Series 7 namespace by using the Cognos Finance Network API Service. You can also export data and metadata from Cognos Finance for use in Framework Manager.

Cognos Controller

You can access Cognos 8 to create Cognos Controller Standard Reports by using a predefined Framework Manager model that is created when Cognos Controller is installed. You can also access published Controller data and structures in Framework Manager for custom reporting and analysis. Both Cognos Controller and Cognos 8 BI must be at the same version.

Transformer

You can use Cognos PowerCubes and Transformer models that were generated by Transformer 7.3 or later directly in Cognos 8. The cubes and models are upwards compatible and require no migration or upgrade tools. You can run reports and analyses in Cognos 8 against the Cognos PowerCubes.

If you want to use the new integration features of Transformer with Cognos 8, you can upgrade Cognos Series 7.x Transformer models to Cognos 8 BI Transformer 8.3. This allows you to use Cognos 8 data sources (such as published packages), list reports authored in Query Studio or Report Studio, authenticate using Cognos 8 security, and publish directly to Cognos Connection.

Before you load the model, the Cognos Series 7 namespace must be configured in Cognos 8. The name ID that is used to configure the namespace in Cognos 8 must match the name used in Cognos Series 7. For more information about configuring a Cognos Series 7 namespace in Cognos 8, see the *Installation and Configuration Guide*.

For more information about upgrading Cognos Series 7 secured PowerCubes, see the Cognos 8 Transformer *User Guide*.

For Cognos Series 7 PowerCubes to be used in Cognos 8, we recommend that you optimize the cubes for use in Cognos 8 by using the pcoptimizer utility, which is supplied with Cognos 8. Otherwise, PowerCubes that were created with previous versions of Transformer may take too long to open in the Cognos 8 Web studios. This optimization utility is suitable for older PowerCubes when the model no longer exists or the data used to build the PowerCube is no longer available. It is not necessary to run this command line utility for cubes created in Transformer 8.3. For more information about optimizing PowerCubes, see the Transformer *User Guide*.

You can publish PowerCubes using Transformer 8.3, Framework Manager, or directly in the Cognos 8 portal. You can publish single PowerCube data sources and packages to Cognos Connection interactively in Transformer or in the command line. You can also publish silently using batch scripts after building a PowerCube. A user who has privileges to create data sources and packages in Cognos Connection can publish PowerCubes in Cognos Connection as well. The MDC file must be in a secured location that the Cognos 8 dispatcher can access. Packages that use multiple

PowerCubes or PowerCubes mixed with other data sources should be published using Framework Manager.

If you use a Cognos Series 7 PowerCube as a data source, Cognos 8 converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube.

Data Manager

Data Manager is used to create data warehouses and data repositories for reporting, analysis, and performance management. When Data Manager is installed in your Cognos 8 environment, you can use the Data Movement Service to run builds and JobStreams in Cognos Connection. You must install the Data Manager engine in the same location as your Cognos 8 Application Tier Components. Both Data Manager and Cognos 8 BI must be the same version.

Cognos 8 Go! Mobile

With Cognos 8 Go! Mobile you can access reports authored with Analysis Studio, Report Studio, and Query Studio on a mobile device (such as a BlackBerry®). To download, view, and interact with reports, Cognos 8 Go! Mobile requires the installation of a custom-built, rich client on the mobile device, in addition to the Cognos 8 server components. Both Cognos 8 Go! Mobile and Cognos 8 BI must be at the same version.

Cognos 8 Go! Search

The Cognos 8 Go! Search add-on provides enhanced search and navigation options in Cognos 8. In Cognos Connection, you can use full-text search to locate content. In Analysis Studio, Query Studio, and Cognos Viewer, you can use full-text search and automatic navigation, which locates content related to the content in the current view. The Cognos 8 content store must include content that can be indexed. Both Cognos 8 Go! Search and Cognos 8 BI must be at the same version.

Cognos Series 7 Content That Can Be Recreated in Cognos 8

Some Cognos products cannot be programmatically migrated or upgraded with the migration or upgrade tools for Cognos 8. Cognos 8 offers two options for duplicating content or functionality for the products described below: use the Upfront portal in the Cognos 8 portal or duplicate queries, visualizations, or objects by using Cognos 8 studios.

Cognos Query

You can use the migration tools to identify Cognos Query objects in the Cognos Series 7 migration source. You can then duplicate most Cognos Query functionality in Cognos 8. Foundation queries are available in Cognos 8 when you migrate an Architect model. You can also manually replicate saved queries using SQL components in Report Studio.

Cognos Visualizer

You can duplicate functionality by using the charting, layout, and formatting options in Report Studio and Analysis Studio.

Cognos NoticeCast

You can duplicate alert and notification functionality by using Event Studio and other Cognos 8 components.

Cognos Web Services

You can duplicate most Cognos Web Services functionality using the Cognos 8 Software Development Kit.

CognosScript

You can duplicate automation functionality using the Cognos 8 Software Development Kit.

Cognos Portal Services

You can duplicate most Cognos Portal Services functionality using Cognos Connection.

Chapter 7: Performance Planning

Performance is a measure of how effectively a system completes the tasks it was designed to accomplish. It is a function of processing capacity and workload. A system that performs well

- has the capacity to process requests quickly

  Decide how much hardware you need to run Cognos 8, given your expected processing workload.

- scales to accommodate an increasing workload

  Decide how much hardware you need to run Cognos 8, given your expected processing workload.

- is available, even in exceptional situations

  Decide how much hardware you need to run Cognos 8, given your expected processing workload.

To ensure that Cognos 8 performs optimally, plan your Cognos 8 implementation with performance in mind. Planning for performance is part science, part art. It involves assessing the needs of different types of users, making decisions based on available resources, and developing a solution that considers security, application integration, and other factors.

This section does not provide absolute rules for planning Cognos 8 performance. It describes variables that affect performance, and ways to consider them when implementing Cognos 8. The variables include the following:

- capacity (p. 70)

  Decide how much hardware you need to run Cognos 8, given your expected processing workload.

- scalability (p. 75)

  Decide how to install and configure Cognos 8 components to take advantage of the ability of Cognos 8 to scale to meet increasing demand.

- availability (p. 81)

  Decide how to implement Cognos 8 to take advantage of its ability to provide failover support in the event of a hardware failure or another system anomaly.

Maintaining Cognos 8 performance is an ongoing task. After implementing Cognos 8, monitor and tune performance regularly. For information, see "Performance Monitoring and Tuning" (p. 85).

Capacity Planning

Planning for capacity means determining the hardware needed for your system to perform well under its anticipated workload.

Capacity planning is a challenge, because it involves many variables, some of which are difficult or impossible to measure. It is the science of measuring known variables and developing an educated estimate of resource requirements on the basis of those measurements. It is also the art of allowing for unknown variables and assessing their impact on the estimates derived from the known variables.

To determine your Cognos 8 capacity requirements, gather information about the following:

- Cognos 8 users

  Estimate the number of Cognos 8 users you expect to have, and when you expect them to use Cognos 8.

- application complexity

  Assess the complexity of the processing that your users will demand of Cognos 8.

- your infrastructure

  The characteristics of your environment and infrastructure.

Capacity planning is an ongoing process. After implementing Cognos 8, monitor and modify your capacity as necessary to meet your performance expectations.

Estimating Cognos 8 User Load

In general, the greater the number of users, and the more concentrated their requests over time, the more hardware you need for a system to perform effectively. As a result, when planning adequate capacity for Cognos 8, you should estimate the number of people who will use Cognos 8 and determine when they will use Cognos 8. This can help you decide not only how much hardware you need, but also how to make the best use of the hardware you have.

Estimating Concurrent Users

The only users placing load on Cognos 8 are those who are actually performing processing. These are concurrent users. You can estimate the number of concurrent users, based on your total user population, by distinguishing between named, active, and concurrent users:

- named users

  Named users are all of the users authorized to use Cognos 8; that is, your total user population.

- active users

  A subset of named users, active users are logged on to Cognos 8 and can demand system resources.

- concurrent users

  A subset of active users, concurrent users are simultaneously demanding system resources. This includes users submitting requests and users waiting for a response to a request.

As a general rule, the ratio of named to active to concurrent users for business intelligence applications is about 100:10:1. In other words, for every 1000 named users there are 100 active users and 10 concurrent users.

The concurrency ratio can vary over time, and is affected by many factors. For example, the number of concurrent users relative to active and named users tends to be higher when the user population is small. However, the most important determinant of the concurrency ratio is how processing demand is distributed over time.

Estimating Load Distribution

In Cognos 8, load is generated by

- user navigation and processing requests, such as requests to run or view reports
- requests made through automated or event-driven processes, including scheduled and burst reports

By determining when users are most likely to be using Cognos 8 and submitting processing requests, you can decide when to schedule automated processes. This allows you to distribute the processing load evenly over time, so that you make the best use of your system resources to maintain optimal performance. The key to doing this is estimating the number of concurrent users that will be applying load to your Cognos 8 system at any time.

Factors such as business hours, business practices, and the geographic distribution of users can determine how the concurrency rate changes over time, and how you choose to ensure adequate capacity.

A business intelligence application in which requests are spread evenly throughout the day has a lower peak concurrency ratio than an application in which the majority of requests are limited to a specific time of day. For example, if users are concentrated in one time zone, there will likely be heavy demand during business hours, followed by a period of low demand after hours. In this situation, you may be able to manage peak and non-peak time periods by sharing hardware resources between interactive and noninteractive processes. You would schedule automated activity to run in non-peak times to produce content for retrieval by interactive users in peak times.

On the other hand, if your user population is distributed across several time zones, user load on the system tends to be spread out over more hours, and there are fewer available non-peak hours for scheduled activities. In this situation, you may choose to dedicate separate hardware resources for interactive and noninteractive use.

Scheduling Processing to Distribute Load

Knowing how user load is distributed helps you decide when to schedule automated processes. Scheduling can be applied to two types of reports:

- scheduled reports

  These reports often depend on updated, event-driven information, such as sales data for the previous day.

- burst reports

These are reports for which multiple users require filtered data based on a predetermined schedule. Burst reports are used when a common report format is applicable to more than one recipient, but each recipient requires customized information.

Scheduling is most useful for reports based on data that is updated on a predictable and cyclical basis. For example, an organization may need to produce sales reports based on information from the previous day, and make them available to users at the start of each business day. If users generate these reports at the beginning of each day, it creates considerable load on the system. By scheduling the reports to be triggered by data refresh, and run during non-peak times, the capacity required at peak times is reduced.

For information about tuning report scheduling and bursting after Cognos 8 is implemented, see "Cognos 8 Tuning" (p. 88). For information about how to schedule reports, see the *Administration and Security Guide*.

Assessing Application Complexity

Load is not only determined by the number of concurrent users, but by the complexity of their processing requests. The greater the complexity of a request, the more time is needed to process the request. In general, hardware resources can process more requests in a given time period when the requests are simple rather than complex. As a result, application complexity is an important determinant of the number of concurrent users that can be supported on a given hardware infrastructure.

The complexity of a Cognos 8 application depends on such things as the amount of work required to process the result set returned from the database query, and the size and layout of the report output. Size is determined by the number of pages in a report and the presence of elements, such as charts.

By identifying reports run at peak times, and improving their efficiency while meeting user requirements, you can improve performance during peak times. Because reporting patterns change over time, assessing application complexity, and improving reporting efficiency, should be ongoing activities. For more information, see "Performance Monitoring and Tuning" (p. 85).

Planning Infrastructure Components

Cognos 8 performance also depends on the characteristics of your infrastructure.

Ideally, Cognos 8 server components should be connected by a network with 100 Mb of available capacity. Network bandwidth between a Web browser and a Web server does not affect system scalability, but does affect user performance.

Use true server computers, rather than fast workstations. True server computers run business applications faster and provide systems that are less likely to fail.

Will Web and application servers be dedicated solely for use by Cognos 8, or shared by other software products? If other applications are sharing the resources, these applications must be taken into account when determining capacity requirements.

Install only gateway components on server computers that are dedicated to Web server processing. Web servers are designed to handle many small requests. Application servers often handle larger requests.

Use the gateway type most appropriate for your environment. For example, for some environments, ISAPI or Apache may provide better performance than CGI.

The complexity of your security infrastructure can increase response time. As your security infrastructure becomes more complex, a user request must be validated more frequently. For example, if you implement multiple network firewalls, each firewall must validate every request that passes through it. This can increase the time taken to complete the request. In addition, if you use SSL, the overhead of SSL encryption adds both processing overhead and size to the response.

Because notification service generates additional email traffic, ensure that your mail server can scale to support the increased load.

Sizing Your Content Store

The content store is used by Content Manager to store all Cognos 8 information that is visible in, or managed through, Cognos Connection or your third-party portal. The content store is at the heart of Cognos 8, and must have sufficient resources to operate effectively. To maximize Cognos 8 performance and scalability, ensure that your content store has the resources required to ensure that it does not become a bottleneck.

The size of the Cognos 8 content store you need depends on the number and size of the Cognos 8 items, such as reports, packages, and schedules, that you will create and store. Over time, as users create more items, the amount of space needed for the content store typically increases.

When determining the amount of space to allocate for your content store, consider the following:

- number of users

  The greater the number of users, the greater the number of reports typically run and stored, and the larger the content store needed.

- number of saved reports

  The greater the number of reports saved, the larger the content store needed. Reports designed for use throughout an organization, and stored in public folders, are often duplicated by users in private folders. This increases the number of reports stored and the space required for them.

- number of saved views

  The greater the number of report views saved, the greater the space required.

- number of folders

  Cognos 8 typically uses public folders as well as one or more private folders for each user. The number of characters in the name and description of each folder can increase the folder size.

- number of schedules

  Schedules can exist for daily, weekly, and monthly print runs. The greater the number of schedules, the greater the content store space required.

- number of Framework Manager packages

The greater the number of packages, and the number of tables and query subjects in those packages, the greater the space required.

- additional storage items

  Additional storage items, such as transaction logs and temporary space requirements, increase the size of the content store required.

Example - Estimating Content Store Size

The size of an empty content store hosted in a MS SQL Server database is approximately 2 to 3 Mb. Depending on your size allocation strategy, this may vary for other supported databases.

The number of concurrent users affects the size of the content store because temporary disk space is allocated to serve report run requests, even if the requests are not saved.

Out of 50 concurrent users, approximately 25% will be executing reports and 75% will be viewing saved outputs. As a result, approximately 12.5 of the 50 users will be running reports (50 concurrent users * 0.25 executing reports = 12.5 concurrent users).

The following table provides an example of how to estimate the size of the content store you need.

Factor	Number	Estimate of content store requirements (Kb)
Named users	1000*	not applicable
Active users	250*	not applicable
Concurrent users (temp space requirements)	50*	5,000,000
Saved reports: 1-10 pages (2 per user for Public and Myfolder copies at 340 Kb per report)	1001	340,340
Saved reports: 10-100 pages (9 per user for 4 Public and 5 Myfolder copies at 440 Kb per report)	5,004	2,201,760
Saved custom views: 1-100 rows (3 per user, all Myfolders at 250 Kb per view)	3,000	750,000
Saved custom views: 100-1000 rows (8 per user, all Myfolders at 350 Kb per view)	8,000	2,800,000
Folders (Public and Myfolders)	1,025	500
Framework Manager models	15	100,000
Framework Manager models (tables)	25	--

Factor	Number	Estimate of content store requirements (Kb)
Framework Manager models (query subjects)	50	--
Schedules (day and week)	175	5,000
Empty content store	--	3,000
Database transaction logs	--	3,000,000
Total	--	14,200,600
*As a rule of thumb, the ratio of named to active to concurrent users is 100:10:1. However, the ratio varies with the environment. For more information, see "Estimating Concurrent Users" (p. 70).		

For more information about capacity planning, visit the Cognos Support Web site (http://support.cognos.com).

Scalability Planning

Scalability is the ability of a system to adapt to increased processing demands in a predictable way, without becoming too complex, expensive, or unmanageable. As you deploy a system to larger numbers of users, often in different locations and time zones and with different language requirements, scalability becomes increasingly important.

Cognos 8 was designed for scalability. It scales vertically using more powerful computers, and horizontally using a greater number of computers. How you install and configure Cognos 8 components can enhance its scalability.

Web Server and Gateway Scalability

All Web communication in Cognos 8 is through a Cognos 8 gateway installed on a Web server. To increase the scalability of your Cognos 8 system, you can run your Web server on a larger computer. You can also install the Cognos 8 gateway on more than one Web server and configure your servers to leverage load balancing features.

Load Balancing

Load balancing spreads tasks among all available processors. It is important in any system, and is a key to processing capacity and scalability. In Cognos 8, load balancing means ensuring that processing requests are distributed appropriately among all the available Cognos 8 servers. Cognos 8 does this automatically, but you can configure load balancing as well.

Automatic Load Balancing

In a distributed environment, Cognos 8 balances request load automatically. By default, as servers are added to the system, each server dispatcher processes the same number of requests. If there is more than one instance of a given service, the dispatcher distributes requests to all the enabled instances of the service that are registered in Content Manager.

Configuring Load Balancing

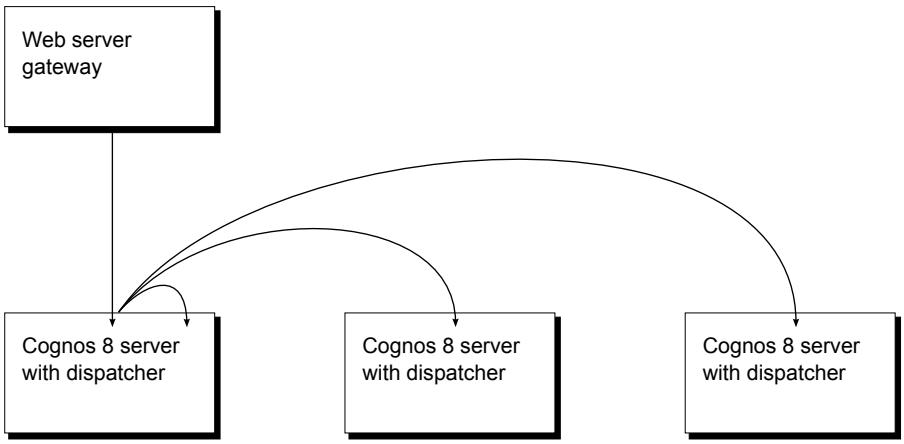
While automatic load balancing may be appropriate when hardware resources are identical throughout a server topology, it may not be ideal in environments containing a mix of hardware resources with different capacity characteristics. In a hardware environment that contains servers with varying degrees of processing capacity, it is desirable to balance the processing load according the server's capacity.

In Cognos 8, you can set process capacity settings using server administration options. For example, if you have two servers, one of which has twice the capacity of the other, you might assign the more powerful server a weight of two and the less powerful server a weight of one. Cognos 8 then submits twice as many requests to the more powerful server.

For more information about Cognos 8 dispatcher settings, see the *Administration and Security Guide*.

Load Balancing Dispatchers

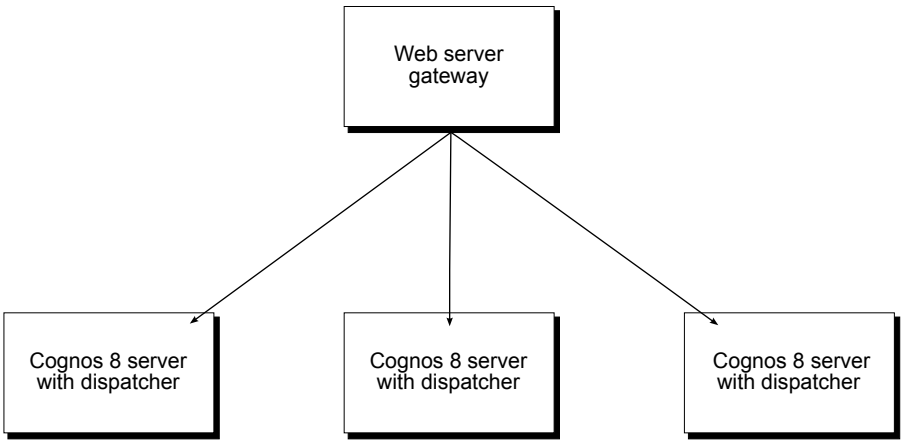
Without a software or hardware load balancing mechanism, each Cognos 8 gateway is aware of only one dispatcher, and distributes all requests to that dispatcher. The dispatcher then distributes the requests among Cognos 8 servers. Because every request initially goes through the same dispatcher on one server, the load on that server is increased. An extra step is needed to automatically balance the load, as shown in the following diagram.



This extra step can be avoided by either implementing load balancing without an external load balancing mechanism, or by using a router or other load balancing mechanism.

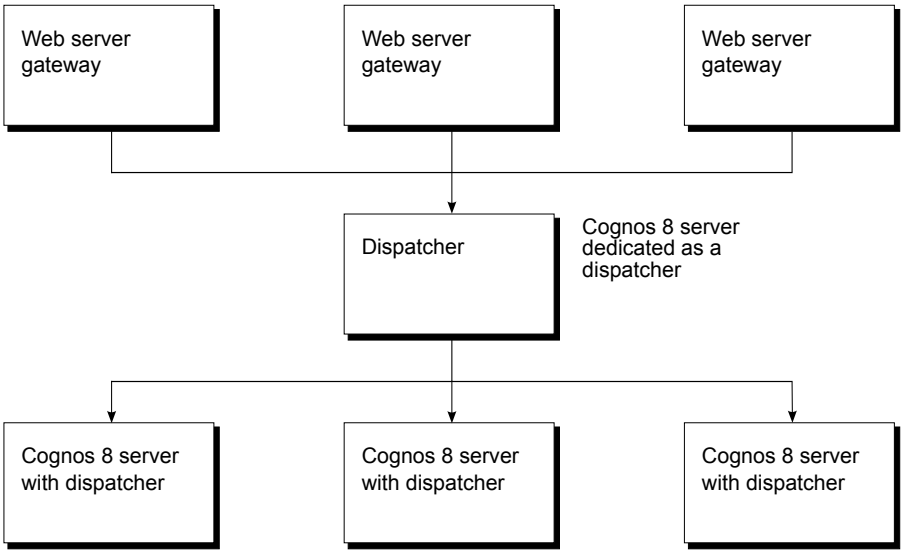
Load Balancing Without an External Mechanism

Since gateway servers often have less load than Cognos 8 servers, you may achieve better performance by configuring dispatchers together with the gateways, as shown in the following diagram.



This ensures that the processing capacity of the Cognos 8 servers is directed toward serving report requests rather than load balancing requests.

You can also achieve load balancing by having gateways direct all traffic to a Cognos 8 server computer that is dedicated to dispatching, as shown in the following diagram.


Web server gateway
Web server gateway
Web server gateway
Dispatcher
Cognos 8 server dedicated as a dispatcher
Cognos 8 server with dispatcher
Cognos 8 server with dispatcher
Cognos 8 server with dispatcher

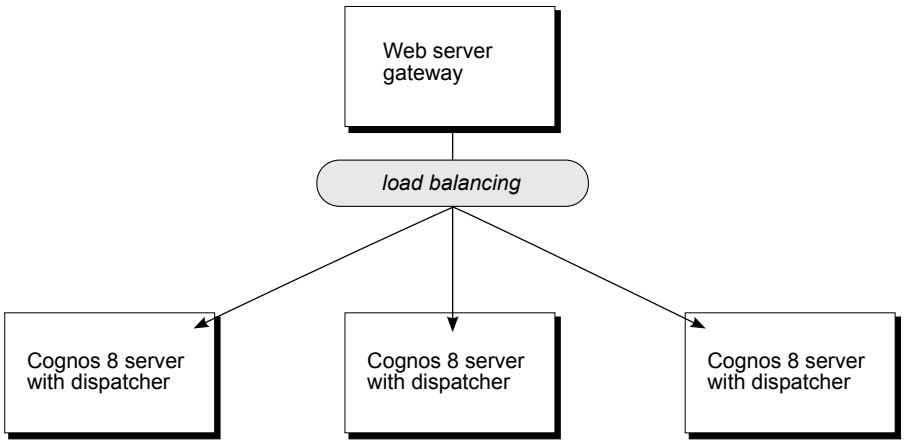
This configuration also removes dispatching load from the Cognos 8 servers. However, it does require separate dispatching computers.

Using External Load-Balancing Mechanisms

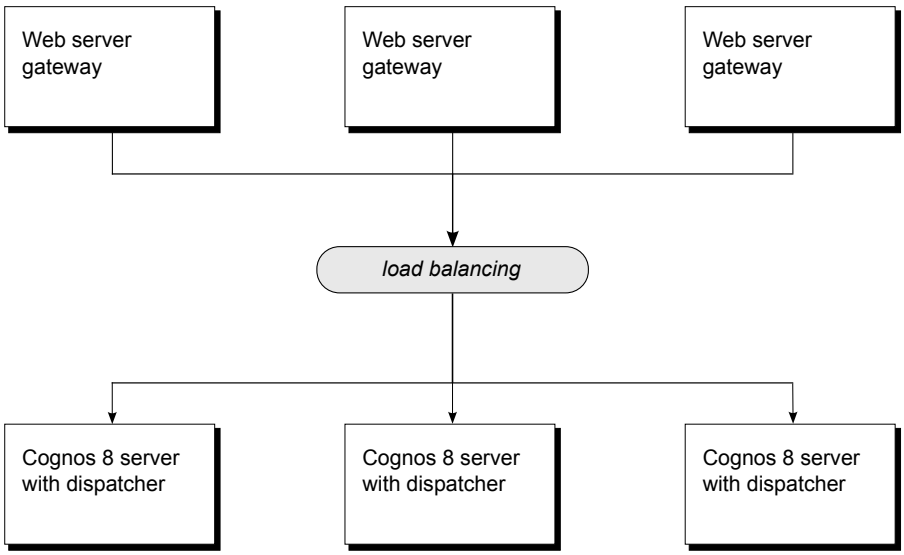
You can use external load-balancing mechanisms, such as routers, to further distribute tasks in Cognos 8. Load-balancing routers can be used in either or both of these locations:

- between the browser and Tier 1: Web Server
- between Tier 1: Web Server and Tier 2: Cognos 8 Server

You can use an external load-balancing mechanism to distribute requests to dispatchers across all available servers, as shown in the following diagram.


Web server gateway
load balancing
Cognos 8 server with dispatcher
Cognos 8 server with dispatcher
Cognos 8 server with dispatcher

You can also use routers with multiple gateways, as shown in the following diagram.



An ideal load-balancing mechanism provides the same capacity awareness as a Cognos 8 dispatcher.

To ensure that requests are not distributed by both an external load-balancing mechanism and the dispatcher, you must configure the dispatchers to not use their built-in load balancing for low affinity requests (p. 78). This ensures that requests remain at the server where the hardware load balancer directed them.

Request Affinity

Affinity refers to whether a request is assigned to a specific server or whether a load-balancing mechanism can assign it to another server. Affinity between request and server ensures that requests are routed to an appropriate computer for processing. Cognos 8 uses the following types of affinity: absolute, control, high, low, session, and server. The cancel operation is handled with a dedicated connection and does not have an affinity type.

To ensure that requests are managed efficiently and load is balanced, Cognos 8 uses request affinity to route some requests. For example, requests are routed back to the Cognos 8 server that handled earlier, related requests. Cognos 8 does this automatically. The use of one or more load-balancing mechanisms does not disrupt request affinity processing.

ReportService connections can be defined as AffineConnections or NonAffineConnections. AffineConnections accept only absolute and high affinity requests. NonAffineConnections accept all types of reportService requests.

Absolute Affinity

Absolute affinity requests are always routed back to the server that processed the original request. If the server is not available, the request fails. For example, when a user cancels a running report, absolute affinity routes the cancel request back to the executing process. Absolute affinity is used to create an association between the client and the executing server to ensure that long-running requests do not time out.

Cognos 8 routes absolute affinity requests to a specific server, regardless of the load balancing used. An absolute affinity request is used with operations such as `getOutput` and `release`.

Control Affinity

Control affinity requests are routed in the same way as absolute affinity requests. A control affinity request is reserved for system operations such as `wait` and `cancel`.

High Affinity

High affinity requests can be processed on any of a number of servers, but resource consumption is minimized if the request is routed back to the executing process. The dispatcher routes a high affinity request to the server that is specified by the conversation context node ID. If the specified server is not available, the request is routed to any available server.

For example, when a pageDown command is run while reading a report, the command can be run most efficiently by using the process that served up the page that is shown. If that process is not available because the administrator shut down the computer or there was a network failure, the request is routed to another available process. The next page can still be served up, although the process will be slower.

Cognos 8 routes high affinity requests to a specific server regardless of the load balancing used. A high affinity request is used with the following operations: `back`, `email`, `firstPage`, `forward`, `lastPage`, `nextPage`, `previousPage`, `print`, `render`, `save`, and `saveAs`.

Low Affinity

Low affinity requests will operate just as efficiently on any computer. For example, a report request can run on any computer in the Cognos 8 system.

A low affinity request is used with the following operations: `add`, `collectParameterValues`, `execute`, `getMetadata`, `getParameters`, `query`, `testDataSourceConnection`, `update`, and `validate`.

For more information about affinity in Cognos 8, see "Setting Affinity Connections" (p. 90).

Session Affinity

Session affinity requests are routed according to the conversation context node ID. If the node ID is present, they are routed in the same way as a high affinity request. If the node ID is absent, they

are routed in the same way as a low affinity request. Session affinity is used with the query reuse feature: when query reuse is turned on and you run a report for the first time, the query is stored in the cache of your current session and reused the next time you run the report. For more information, see the Framework Manager *User Guide*.

Server Affinity

Server affinity requests are routed in the same way as absolute affinity requests.Server affinity is used for data source testing in administration: an administrator can test the connection to a new data source. For more information, see the topic about creating a data source in the *Administration and Security Guide*.

Cognos 8 Server Scalability

The Cognos 8 application server has one or more Cognos 8 servers. Each Cognos 8 installation contains Content Manager to manage data stored in the content store. Each Cognos 8 server contains a dispatcher that runs the Cognos 8 presentation service, batch report and report services, job and schedule monitor service, and log service.

Only one Content Manager is active at a time. The others are on standby. A standby Content Manager becomes active only if the computer on which the active Content Manager is installed fails.

To improve scalability, you can enable or disable Content Manager and the dispatcher services on individual application servers to balance the load for a given computer by request type. For example, if you have three application server computers, you might dedicate one to running interactive report requests, another to Content Manager, and the third to the other Cognos 8 services.

By targeting processing at specific computers in this way, you can control the load on each computer. For example, putting Content Manager on its own computer ensures that other requests do not downgrade its performance by competing for resources. Because report runs tend to be resource intensive, we recommend that you isolate the report services from other activities, especially in larger Cognos 8 deployments. However, before making this type of tuning configuration, analyze your user requirements carefully.

Cognos 8 Services Scalability

Cognos 8 services operate as threads within the dispatcher. The report services differ from the other services in the way they contribute to scalability.

Report and Batch Report Services

The report and batch report services are multi-instance components of Cognos 8. As a result, one or more instances can be configured to operate on each Cognos 8 computer.

The same program is used for both the report service, which handles interactive requests, and the batch report service, which handles scheduled tasks. For information about configuring the number of instances of the report services and the number of threads that each instance handles, see the *Administration and Security Guide*.

Content Manager

Content Manager, which can be installed in Tier 2 or 3 of Cognos 8, stores information in the content store. To allow fast retrieval, Content Manager builds an in-memory cache to service many requests. This ensures optimal performance and enhances scalability by limiting the number of database reads required to meet user requests.

In the single Content Manager process, multiple threads can concurrently service requests for content. Content Manager creates one or more threads for each user request. Performance depends on the power of the central processor unit (CPU) of the computer on which Content Manager is installed.

To increase scalability, use a larger computer capable of managing more concurrent request threads. When scaling up Content Manager, be sure to scale up the content store relational database management system so that it does not impede Content Manager performance.

Other Services

The scalability of the presentation service, job and schedule monitor service, and log service, is primarily dependant on the CPU size and the available memory. These components can be scaled in two ways:

- vertically, by using a larger computer capable of managing more concurrent request threads
- horizontally, by running the services on additional computers

There is no specific configuration to tune these components. However, you can view the load-balancing configuration set by the server administrator to determine how much load is given to each computer running these services.

Availability Planning

Availability is the ability of a system to withstand or recover from exceptional situations, such as a computer failure. All Cognos 8 components have built-in failover features to ensure that Cognos 8 handles exceptions well.

You can configure components in each of the Cognos 8 tiers to enhance availability. As a general rule, make all Cognos 8 components available on at least two computers. If the computer on which a Cognos 8 component is running fails, another computer takes over.

If, for tuning reasons, you are not running all Cognos 8 components on every Cognos 8 server, ensure that each component is running on at least two servers. In the event of a computer failure, the remaining component processes requests. Performance may degrade, but there will be service.

Cognos 8 Gateway Availability

All Web communication in Cognos 8 is through a Cognos 8 gateway installed on a Web server. Each gateway can communicate with a single dispatcher in the applications tier.

We recommend that you use two or more Web servers with Cognos 8. This ensures that the failure of a single server does not result in the loss of Cognos 8 service. You can also use an external

load-balancing mechanism, such as a router, to distribute requests across all available dispatchers (p. 75).

In the unlikely event of a failure, the Cognos 8 gateway and Cognos Application Firewall are restarted automatically by the Web server.

Cognos 8 Server Availability

The Cognos 8 server contains Content Manager to store and manage information, and a dispatcher to start Cognos 8 services and route requests.

The dispatcher manages the Cognos 8 presentation service, batch report and report services, job and schedule monitor service, and log service. To ensure that the failure of one computer or service does not cause Cognos 8 to become unavailable, install two or more Cognos 8 servers. You can distribute services across Cognos 8 servers, and you do not need to enable all services on all Cognos 8 servers.

The Java technology of the Cognos 8 server provides Content Manager and the dispatcher with built-in failover support. Both components are multithreaded, and the threads are isolated from each other. If a failure occurs, it affects only a single request thread. If that thread is lost, no other threads are affected, and the failure does not affect the service as a whole.

If Content Manager or the dispatcher fails, the Cognos 8 server restarts it automatically. If you use the Apache Tomcat servlet container provided with Cognos 8, the Cognos 8 service monitors and restarts Tomcat. If you use an application server rather than Tomcat, the administration services for that application server restart it.

Content Manager Availability

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby. The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

By default, the first Content Manager installed with Cognos 8 is the active one. A Cognos 8 server administrator can change the default Content Manager and the active Content Manager at any time. When Cognos 8 is started, the default Content Manager locks the content store from access by all other installations of Content Manager. These other Content Manager installations enter standby mode.

This failover mechanism works because dispatchers and the active Content Manager routinely communicate with each other. If a dispatcher can no longer reach Content Manager, the dispatcher signals a standby Content Manager, which becomes the active Content Manager. The other installations of Content Manager remain in standby mode for continuing failover support. The standby Content Managers retrieve cryptographic settings, such as the common symmetric key (used to encrypt and decrypt data), from the active Content Manager.

Content Store Availability

Content Manager stores Cognos 8 information in the content store RDBMS. Content Manager writes to the content store using proper relational transactions. You can use standard database tools for backing up and restoring the content store, and standard database availability mechanisms to protect the content store from failure.

Chapter 8: Performance Monitoring and Tuning

Over time, a Cognos 8 environment changes. User populations grow, processing requests tend to increase in number and complexity, and network capacity and other aspects of infrastructure may be modified.

These changes can affect Cognos 8 performance. As a result, it is important to monitor and tune performance regularly.

Monitoring performance means regularly checking the status of your Cognos 8 installation and its resources. Cognos 8 provides metrics (p. 85) for checking the performance of the system, servers, dispatchers, or services. You can set thresholds for metrics to identify when the performance exceeds or falls short of expected ranges. You can configure the system to notify anyone who should be made aware of the problem when a performance issue occurs.

Tuning can involve adjustments in the following areas:

- databases (p. 87)

  Keep your databases optimized for querying and reporting.

- application servers (p. 87)

  Adjust your application server memory and connection settings as required for better performance.

- Web servers (p. 88)

  Tune your Web server for maximum performance.

- Cognos 8 (p. 88)

  Monitor and tune various aspects of your Cognos 8 system.

Perform additional tuning as required. This can involve modifying PDF rendering settings, changing low bandwidth connections, performing regular disk maintenance, and other tasks.

After a certain point, performance tuning efforts yield diminishing returns. A growing user population, and increased processing demands, will eventually require you to consider increasing system capacity. To improve Cognos 8 performance, you can scale vertically by using more powerful servers, or scale horizontally by adding servers and balancing the processing load among your servers. For more information about determining Cognos 8 capacity requirements, see "Capacity Planning" (p. 70). For information about other tuning and maintenance tasks, see the *Installation and Configuration Guide*.

Performance Metrics

You can monitor current system performance using metrics. You can assess the status of the system as a whole, as well as the status of individual servers, dispatchers, and enabled services.

For example, you check the performance metrics and notice that the report service shows a red square indicator, which identifies poor performance. You view the metrics for the report service and determine that the number of requests waiting in the queue exceeds the number that can be processed in a specified length of time. You can then take action to reduce the number of requests waiting in the queue.

Metrics are grouped using the following categories:

- session metrics for monitoring the number of sessions in your system

  These metrics are collected by Content Manager.

- queue metrics for monitoring the ability of dispatchers and services to keep up with requests that are waiting in queues

  For example, queue metrics for services may identify that requests are waiting too long in a queue for processing. There are two types of queue metrics. Global queue metrics, which include the JobQueue, SMTP Queue, and Task Queue, are collected by the monitor service. Service queue metrics are collected by individual services.

- JVM metrics for monitoring status information such as the length of time a JVM in the Cognos 8 environment has been running and how much memory it is using

  These metrics are collected by the JVM.

- service request metrics for monitoring processing times, volume of requests, operational status of services, and response times

  These metrics are collected by the dispatcher that manages the service.

- report service metrics for monitoring report service processes

  These metrics are collected by the dispatcher that manages the report service.

The availability of a metric depends on the resource with which the metric is associated. For example, some metrics are available for the system, servers, dispatchers, and services. Other metrics may be available for only a subset of these resources.

You define the threshold values that determine whether the status for a resource indicates excellent performance (a green indicator), average performance (a yellow indicator), or poor performance (a red indicator). There are no default threshold values. If you define thresholds, the values are stored in the content store.

You can also create an agent that monitors the metrics and notifies you when threshold values are exceeded. For example, you can create an agent that sends you an email when a threshold value is exceeded.

When a threshold is exceeded, the dispatcher writes an entry to the logging database.

For information about system metrics, including how to define threshold values and notifications, see the Cognos 8 *Administration and Security Guide*.

Database Tuning

The data source used by Cognos 8 is usually a relational database management system, such as IBM DB2, Microsoft SQL Server, or Oracle. To ensure that Cognos 8 continues to perform well, it is important to maintain the performance of your database. This means optimizing it for querying, reporting, and analyzing. If Cognos 8 and other applications demand more of a database than it can provide, or queries are too large for a database to handle efficiently, you may experience increased response times and degradation in Cognos 8 performance and scalability.

For information about tuning your database, see the documentation provided by your database vendor.

Application Server Tuning

The Cognos 8 Java application server contains the Content Manager servlet and dispatcher servlet. By default, Cognos 8 installs and uses Tomcat as the default application server. You can also configure Cognos 8 to use another Java application server.

Regardless of the application server you use, to enhance and maintain Cognos 8 performance, you should monitor memory settings and connection limits and tune them based on Cognos 8 usage characteristics.

Changing Memory Settings

The memory settings of your application server dictate the memory that is available to Cognos 8 dispatchers and services managed by the Java servlet.

In Cognos Configuration, the default memory allocation is 768 Megabytes. If you expect many users and report requests, you may want to increase the memory allocation beyond the default.

The memory allocation strategy for your application server depends on the available capacity of your resources, and on the resource needs of other applications running on the server. In general, we recommend that you configure your application server with a minimum of 512 Megabytes of memory for multi-user applications. You may be able to reduce application server memory to 256 Kilobytes, but you should only consider this for single users, or for proof of concept or demonstration applications.

To configure Apache Tomcat memory settings, use Cognos Configuration or alternative methods. For information about using Cognos Configuration, see the *Installation and Configuration Guide*. If you use an application server other than Tomcat, consult the documentation for that product.

Setting Connection Limits

For the Cognos 8 dispatcher to service the expected number of requests, it is important to configure the connection limits of your application server. Depending on your application server, connections may be referred to as threads. The setting applied will determine the number of available connections, or threads, that can be handled simultaneously by the application server process.

To configure Apache Tomcat connection settings, use the \conf\server.xml file located in the Tomcat directory in your Cognos 8 installation location. Cognos 8 uses the settings for the coyote connector.

If the value of this application server setting is too low, users may encounter difficulties when making Cognos 8 requests. It is a good practice to monitor the application server process and its use of connections.

Web Server Tuning

The default Cognos 8 gateway is CGI, which can be used with all supported Web servers. For improved performance, consider using a scalable gateway, such as Apache mod for Apache and IBM HTTP servers, or ISAPI for IIS Web servers.

For information about Web server scalability in Cognos 8, see "Web Server and Gateway Scalability" (p. 75). For information about tuning your Web server, see the documentation provided by your Web server vendor.

Cognos 8 Tuning

The way that you use and configure Cognos 8 can affect its performance. For example, you can design models and reports with performance in mind, configure Cognos 8 dispatchers and services for performance, and schedule jobs to make the best use of system resources.

Designing Models and Reports for Performance

Designing and creating models in Framework Manager is an important step in the Cognos 8 workflow (p. 48). A model specifies, structures, adds to, and manages the metadata used to create reports. For optimal Cognos 8 performance, a modeler can design models that specify default prompting, and that set the query processing type.

Specifying Default Prompting

Models can include reports that prompt the user with a descriptive name while filtering on a code or key value for improved query performance.

You can modify a model to ensure that queries sent to the data source are efficient, well formed, and secure. To ensure optimal performance, the Framework Manager modeler can

- specify the rules governing query generation
- restrict user access to specific rows or columns of data
- model data relationships to hide the complexity of data from report authors

For more information, see the Framework Manager *User Guide*.

Setting Query Processing Type

For relational metadata, you can improve performance by selecting the right type of query processing.

There are two types of query processing:

- limited local

  The database server does as much of the SQL processing and execution as possible. However, some reports or report sections use local SQL processing.

- database only

  The database server does all the SQL processing and execution. An error appears if any reports or report sections require local SQL processing.

Although the database server can usually run the SQL and run reports much faster, local processing is sometimes necessary. For example, choose limited local processing if you want to create cross database joins or if you want report authors to use unsupported SQL99 functions.

Some complex queries, such as a query that must generate an `At` clause to avoid double-counting, require limited local processing. In this case, the query automatically uses limited local processing even if the package was published with database only processing.

For more information, see the Framework Manager *User Guide*.

Tuning Cognos 8 Dispatchers

Cognos 8 dispatchers manage the distribution of requests. You can monitor Cognos 8 dispatchers using administration options (p. 14).

In a distributed Cognos 8 environment, there are two or more servers, each with a dispatcher to manage the Cognos 8 request flow. The dispatcher is responsible for routing requests to the services configured on a particular Cognos 8 server.

A Cognos 8 server can be configured to handle a specified proportion of requests. This is especially important if you have servers of different capacity and must make granular changes to specific servers in your environment.

Setting the Process Capacity

Each Cognos 8 dispatcher is assigned a process capacity. It dictates the number of requests that will be handled by a server. By default, request distribution uses a weighted round-robin algorithm that distributes requests equally among all configured dispatchers. In this case, the process capacity for each dispatcher is assigned a weight of 1.0.

The process capacity should be configured according to the relative performance of each server. For example, consider a two-server topology. If all other variables are constant, a quad-processor server should be configured with a processor capacity of 2.0, and a dual-processor server given a processing capacity of 1.0. This means that in the two-server topology, one server receives twice the number of requests as the other.

For more information, see the *Administration and Security Guide*.

Specifying Advanced Dispatcher Routing

Depending on how your system is set up, you may want to control how reports are distributed among servers. For example, you have different departments that maintain their own servers, or

you have specific servers set up for specific data access, such as Windows server for Microsoft SQL Server databases and Linux servers set up for DB2 access. You can set up Cognos 8 so that report requests are processed by specific servers by applying routing rules to specific packages, groups, and roles.

For more information, see the *Administration and Security Guide*.

Tuning the Report Service, Batch Report Service, and Report Data Service

The report service, batch report service, and report data service have several settings that you can configure to optimize the use of resources.

There are a number of processes associated with the report service (p. 20) and the batch report service (p. 20). When these services receive requests from the dispatcher, they start processes to handle the requests. You can specify the maximum number of processes that these services can start at any one time.

The number of processes should be configured based on the amount of available capacity provided by Cognos 8 servers. In general, report processing is a CPU-bound process. As a result, the number of CPUs in a server, and the clock rates of those CPUs, are the main variables to keep in mind when adjusting this setting from the default value of 2.

For example, a server with four available CPUs should generally be configured to use more batch report service processes than a server with only two available CPUs. Similarly, given two servers with an equal number of CPUs, the server with a significantly faster CPU clock rate should be configured to use more batch report and report service processes.

For the report data service (p. 20), you can specify the maximum report size that can be sent.

For more information about server administration settings, see the *Administration and Security Guide*.

Setting Affinity Connections

You can specify the maximum number of high affinity and low affinity connections that the dispatcher can open to handle requests. High affinity connections are used to process absolute and high affinity requests from the report services, while low affinity connections are used to process low affinity requests.

High Affinity Connections

High affinity requests apply to the report service only, and not to the batch report service. A high affinity connection is used to handle a high affinity request, and each connection handles one request at a time. A high affinity request is a transaction that can benefit from a previously processed request. It can be processed on any of a number of servers, but resource consumption is minimized if the request is routed back to the report service process that was used to execute the original process.

Each report process has a configurable number of high affinity connections. The number of high affinity connections to set should be based on the number of low affinity connections set for each report process, as well as the capacity required for other services on the same server.

The distribution decision between high and low affinity connections per batch report process should be a function of the anticipated distribution of request types. For example, an HTML reporting application may have a greater likelihood of high affinity requests than a PDF reporting application. The page down request for an HTML report uses a high affinity connection whenever possible.

In general, we recommend that the number of batch report service and report service processes should be the primary parameter to be optimized when deploying a Cognos 8 application. After system resource use is configured to operate efficiently, the number of affinity connections can be tuned for further optimization.

Note: If the number of affinity connections per process is set too high, the process may be overburdened with managing connections. This will result in competition for system resources, and requests will take longer to complete due to inefficient use of server resources.

Low Affinity Connections

A low affinity connection is used to handle a low affinity request. Each connection handles one request at a time. A low affinity request will operate just as efficiently on any server.

Both the report service and batch report service are capable of handling low affinity requests. Low affinity requests that have been initiated by scheduled activity will make use of the low affinity connections configured for a batch report service. Low affinity requests that have been initiated by user-driven activity will make use of the low affinity connections configured for a report service.

Each report and batch report process has a configurable number of low affinity connections. The number of low affinity connections per report service process should be set in coordination with the settings specified for the batch report service.

The distribution decision between high and low affinity connections per process should be a function of the anticipated distribution of request types. For example, an HTML reporting application may have a greater likelihood of high affinity requests than a mainly PDF reporting application. The page down request for an HTML report uses a high affinity connection whenever possible.

In general, we recommend that the number of report service and batch report service processes should be the primary parameter to be optimized when initially deploying a Cognos 8 application. Once system resource use is configured to operate efficiently, the number of affinity connections can be tuned for further optimization.

Note: If the number of affinity connections per process is set too high, the process may be overburdened with managing connections. This will result in competition for system resources and requests will take longer to complete due to inefficient use of server resources.

Affinity Level of Cognos 8 Activities

Cognos 8 includes the following high affinity activities:

- Report Viewer links
  - Run again
  - Return
- HTML report navigation

    - Top page
    - Page up
    - Page down
    - Bottom page
- delivery options
    - Save
    - Save As
    - Print
    - Email
    - Viewing

Cognos 8 includes the following low affinity activities:

- report querying
    - reporting
    - report processing
- report authoring
    - metadata retrieval
    - query validation
- administrative
    - testing data source connections
    - adding objects (folders, jobs, schedules, etc.)
    - refreshing portal page

For more information about affinity, see "Request Affinity" (p. 78). For information about setting affinity connections, see the *Administration and Security Guide*.

Best Practices for Scheduled Reporting

The Cognos 8 architecture differentiates between the processing of interactive and noninteractive requests. All requests that are initiated through user activity are processed by the report service, while scheduled or event-driven activity is processed by the batch report service.

Scheduled reporting is a critical aspect of any large-scale enterprise reporting solution. The effective management of low or noninteractive usage time periods, in combination with an organization's data refresh cycles, provides an opportunity for administrators to prepare as much information as possible during off-peak times for later retrieval by the greater business intelligence user community.

Using Jobs to Schedule Reports

Reports can be scheduled on an individual basis. However, if you have many reports to schedule, scheduling on a one-by-one basis can become burdensome. As an alternative, you can use jobs to execute scheduled activities.

A job is a container of scheduled processing activities that operates in a coordinated manner. Instead of scheduling individual reports, a job allows multiple reports to execute using the same schedule. Each activity within a job is given a sequence ordering, which is based on how the job was selected.

Jobs can be submitted to run as follows:

- all at once

  All activities in a job will execute simultaneously. This execution strategy is particularly useful when the number of activities within a job (or multiple jobs) is less than the total number of low affinity connections available during the execution period.

- in sequence

  The activities in a job will execute one at a time, based on their sequence ordering. This execution strategy is particularly useful when the number of activities within a job (or multiple jobs) is more than the total number of low affinity connections available during the execution period. In this case, batch report throughput can be maximized by setting an equal number of jobs as available for low affinity connections. The number of activities per job would be set up so that the total number of activities results in the completion of the batch reporting requirements.

Job and Scheduling Service Settings

All scheduled activity is managed by the job and scheduling service. The job and scheduling service is directly related to the batch report service, and should be considered in tandem with that service.

Settings for the job and scheduling service include the following:

- Maximum Jobs During Non-Peak Period

  The maximum number of jobs during non-peak periods identifies a configurable limit to the number of jobs that can simultaneously execute during the specified non-peak period range.

- Maximum Jobs During Peak Period

  The maximum number of jobs during peak periods identifies a configurable limit to the number of jobs that can simultaneously execute during the specified peak period range. If an application does not perform scheduled activity during the specified peak period range, this setting is inapplicable.

For information about these and other job and schedule service settings, see the *Administration and Security Guide*.

Best Practices for Report Bursting

Report bursting is a method of producing a set of reports containing personalized content that is based on a common report definition. Bursting performs a single execution of a report; sections the

content as required, typically based on security access; and distributes the sections to the appropriate users based on report content.

Bursting is a critical aspect of any large-scale enterprise reporting solution. The effective management of low or noninteractive usage time periods, in combination with an organization's data refresh cycles, provides an opportunity for administrators to prepare as much information as possible for later retrieval by the greater business intelligence user community. Report bursting in Cognos 8 streamlines information distribution. A report is created once, and separated out into multiple filtered report outputs that contain individualized content.

Report bursting offers scalability benefits and helps in the effective management of resources. It also reduces network traffic, minimizes database queries, and enables Cognos 8 to process multiple personalized reports in parallel.

Report bursting can be driven interactively or through batch activity. By default, report bursting is configured to use one thread for querying and three threads for report assembly using the raw data returned from a report bursting query. Depending on the amount of hardware available, resource use during a burst is influenced by the number of threads configured. Each thread used for assembling personalized reports can typically use one processor.

Depending on the available capacity of a server, and on the overlap of burst reporting with other forms of processing, it may be beneficial to adjust the default report bursting thread model. For example, if a single report is being burst, and no other processing activity is being performed on a server, it is best to allocate as many threads for report assembly as there are available processors.

The report bursting assembly thread model can be configured to optimize resource use. In the rsvpproperties.xml file located in the *c8_location*/configuration directory, edit the BurstThreadPoolSize property:

```
<property>BurstThreadPoolSize</property>
<value type="long">3</value>
```

For information about using the rsvpproperties.xml file, see "Advanced Report Processing Configuration Settings" (p. 96).

PDF Rendering

You can change PDF rendering settings to improve response time. If a user views a one-page document on an idle system, the CPU time is often less than one second. However, PDF files vary in size, and response time is limited by your network speed.

To improve response time, you can do the following:

- Turn off font embedding.

  Embedding fonts can add 100 Kilobytes or more to each report. Where connection speeds are 56 Kbps or less, we recommend that you turn off font embedding.

- Avoid uncommon fonts.

  When you turn off font embedding, report authors should avoid using any fonts that report consumers may not have installed on their computers. If report consumers do not have the font set used by report authors installed on their computers, a default font is substituted.

- Enable linearized PDF documents.

  You can enable linearized PDF viewing, known as byte serving, which delivers documents to your users as the pages become available. This is enabled by default in the PDF rendering settings and Adobe Acrobat Reader.

For more information about PDF documents, see the documentation provided with Adobe Acrobat.

Low Bandwidth Connections

If you have users who access Cognos 8 using a dial-up connection, we recommend that you change PDF rendering settings to improve performance.

You can also reduce default page sizes in Query Studio and Report Studio. In heavy volume installations, the amount of HTML generated can be high. You can improve performance by lowering the default page size to reduce the amount of HTML initially passed back to the Web server and on to your users.

Disk Maintenance

Over time, data on a physical disk becomes fragmented, which can cause performance degradation when writing to or accessing from the disk. Disk defragmentation should be a regular system maintenance activity.

Monitoring Cognos 8 Servers

You should conduct regular and targeted monitoring of the Cognos 8 servers. This is important to assess the occurrence and impact of paging, memory use, and other measures of an efficient system.

Temporary Space for Cognos 8 Servers

Cognos 8 servers use a variety of directory access depending on the type and amount of activity. For running reports, Cognos 8 servers frequently use temporary space. We recommend that the Cognos 8 temporary space be hosted on a physical disk that is separate from other Cognos 8 directory locations. This maximizes parallel disk access and avoids the unnecessary sequential access that is common when only a single disk device is used.

Reducing Disk Use

Depending on the size of reports and the amount of available memory, Cognos 8 may access a physical disk when processing reports. To improve performance, you can ensure that report processing uses available memory rather than disk space.

Using memory instead of disk space is particularly beneficial in cases where temporary files are created on Cognos 8 servers, causing information transfer from memory to disk. You can monitor

the occurrence of temporary files using the *c8_location*\temp directory. Monitor this folder during report processing periods to determine whether temporary files are created as cclvpage*.tmp.

To ensure that Cognos 8 uses memory instead of disk space, in the rsvpproperties.xml file, edit the VirtualMemoryDiagnostics property to use unlimited memory (value = 2) rather than limited memory (value = 0):

```
<property>VirtualMemoryDiagnostics</property>
<value type="long">2</value>
```

Note: Remove the comment to enable the VirtualMemoryDiagnostics property.

For information about using the rsvpproperties.xml file, see "Advanced Report Processing Configuration Settings" (p. 96).

Advanced Report Processing Configuration Settings

By default, Cognos 8 is configured to process reports and other business intelligence transactions using a standard model applicable to all applications. You can change the default processing behavior for the Cognos 8 server by modifying entries in the rsvpproperties file.

Setting rsvpproperties.xml properties

The rsvpproperties.xml.sample file is located in the *c8_location*/configuration directory. Depending on your specific Cognos 8 application and on the demands placed on it, changing settings in the rsvpproperties.xml file may benefit performance. Examples of settings that can be modified to enhance performance include prompt application, the burst thread model, and virtual memory.

To enable the rsvpproperties.xml.sample file, you must rename the file rsvpproperties.xml and restart Cognos 8. This activity must be conducted on all Cognos 8 servers.

Settings in the rsvpproperties.xml file are very sensitive to change. Changing these properties may greatly impact the behavior of Cognos 8. As a result, you should use discretion when changing these values. For more information, contact Cognos support.

Chapter 9: Globalization Considerations

Many businesses perform transactions in the global market. In this environment, users speak different languages, work in different currencies, use different date and time formats, and expect different sorting orders.

Cognos 8 provides a multinational reporting environment in which users can create reports and access data in different languages. Users can work in the Cognos 8 user interface using their preferred supported language and regional settings, or any combination of supported languages.

Cognos 8 supports both Unicode and non-Unicode data sources. A single installation of Cognos 8 supports multiple languages, and reports can be generated once for use in different languages.

If you will use Cognos 8 in a global environment, decide how to configure Cognos 8 so that interface elements and report contents appear in the languages that users need.

To configure Cognos 8 for a global environment, do the following:

- Ensure that all strings that appear in the Cognos 8 user interface are translated into the required languages.
- Add fonts to your Cognos 8 environment.

  Ensure that the appropriate language packs were installed on all computers in the distributed installation to support the character sets you use.
- Customize language support to the user interface.

  Add or remove user interface language support. You can also specify the language used in the user interface when the language specified in the user locale is not available.
- Ensure that users see reports, data, or metadata in their preferred language.

  You can also specify the language a report is viewed in if the preferred language of the user is not available.
- Customize currency, numbers, dates, and times.

  Ensure that these variables are formatted correctly for users in different locations.
- Configure your database.

  Certain databases require specific configuration of the client or server software to enable multilingual reporting.

For information about installing and configuring Cognos 8, see the *Installation and Configuration Guide*.

Locales

Cognos 8 supports various types of locale. By default, Cognos 8 ensures that all locales, which may come from different sources and in various formats, use a consistent format. That means that all expanded locales conform to a language and regional code setting.

In Cognos 8, a locale specification consists of the following parts, separated by a dash (-):

- The first part is a two-character-set code, such as en, that specifies a language.
- The second part is a two-character-set code, such as us, that specifies a regional setting.

A locale specifies linguistic information and cultural conventions for character type, collation, format of date and time, currency unit, and messages. More than one locale can be associated with a particular language, which allows for regional differences.

Product Locale

The product locale controls the language of the user interface and all messages, including error messages.

Content Locale

The content locale consists of the language and region combinations that are supported for Content Manager objects, Framework Manager objects, Content Manager data formatting, report data formatting, report text (titles), and database data (if the database tool is configured to use locale).

Server Locale

The server locale ensures that all log messages are in one language. It is configured during installation. In a distributed environment, each Cognos 8 server obtains the server locale from Content Manager.

Do not change the server locale after specifying any Cognos groups or roles as part of security modeling within your environment. As well, if more than one Content Manager exists in your Cognos 8 installation, ensure that the server locale is set to the same value for all Content Managers.

Author Locale

The author locale is based on content locale and is the locale used when a report or query specification is created. It determines model binding and literal data formats. Author locales must be supported by the metadata model on which the report is based.

User Locale

Determining the language and locale preferences of users and enforcing an appropriate response locale are important issues when you distribute reports in different languages.

A user locale specifies the default settings that a user wants to use for formatting dates, times, currency, and numbers. Cognos 8 uses this information to present data to the user.

Cognos 8 obtains a value for user locale by checking these sources, in the order listed:

1. authentication provider

If the authentication provider has locale settings that are configured, Cognos 8 uses these values for the user product and content locale.

2. user preference settings

   If the user sets the user preference settings in Cognos Connection, Cognos 8 uses these settings for the user product and content locale and for default formatting options. The user preference settings override the values obtained from the authentication provider.

3. browser cookie

   Anonymous and guest users cannot set user preference settings. For these users, Cognos 8 obtains a user locale from the browser cookie stored on the computer.

Run Locale

Run locale refers to a user product and content locales for a specific Cognos 8 session. Cognos 8 obtains a value for run locale by checking these sources, in the order listed:

1. URL
2. user account object in the content store
3. account information from the authentication provider

   Product locale is used, if specified. Otherwise, content locale is used.

4. language settings in the browser

   Each entry in the locale list for the browser is checked against the product mapping table, and then against the content locale mapping table (p. 102).

5. server locale for the Content Manager computer

Adding Fonts to the Cognos 8 Environment

Cognos 8 uses fonts to render PDF reports on the Cognos 8 server and to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered.

In the case of charts and PDF reports, the fonts must be installed on the Cognos 8 server. For example, if a Cognos Report Studio user selects the Arial font for a report, Arial must be installed on the Cognos 8 server to properly render charts and PDF files. If a requested font is not available, Cognos 8 substitutes a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the personal computer of each Cognos 8 user who will read the HTML report. If a requested font is not available, the browser substitutes a different font.

When creating reports, you must select fonts that your Cognos server or users have installed. Microsoft delivers a broad selection of fonts with different language packs, so this will likely not be an issue in Windows. However, UNIX servers rarely have fonts installed. You should be prepared to purchase and install the fonts you need on both the server and browser clients.

When generating a PDF, Cognos 8 embeds only the glyphs that are used in the report.

If you plan to use different fonts, you must license and install those fonts on each server computer in your authoring environment and production system. You must also ensure that the fonts used in the authoring environment match the fonts used on your Windows and UNIX server computers.

For information about configuring fonts and about mapping substitute fonts, see the *Installation and Configuration Guide*.

Embedded Fonts

To ensure that PDF reports appear correctly in Adobe Reader, Cognos 8 embeds required fonts in reports by default. To minimize the file size, Cognos 8 embeds only the characters (also called glyphs) used in the report rather than all characters in the font set. Cognos 8 embeds fonts only if they are licensed for embedding. The license information is stored in the font itself and is read by Cognos 8.

If you are confident that the fonts used in reports are available on users' computers, you can limit or eliminate embedded fonts to reduce the size of PDF reports. When limiting fonts, you specify whether a font is always or never embedded, using an embedded fonts list in Cognos Configuration.

For more information about limiting embedded fonts, see the *Installation and Configuration Guide*.

Cognos 8 Default Font

If a requested font is not found, the Cognos server renders PDF files and charts using a default font. The default font, Andale WT, is a sans serif font. While it has most of the Unicode characters for many languages, it is not necessarily complete for all languages and does not have the attractive appearance of most purchased fonts. Also, this font has no Glyph Substitution (GSUB) and Ligature support in most languages.

Cognos Report Studio Fonts

Cognos Report Studio is an HTML and JavaScript application that runs in a browser. Because of the browser design, Cognos Report Studio operates within the browser security sandbox and has no access to the list of fonts installed on the local computer. As a result, the list of fonts presented in Cognos Report Studio depends on the fonts installed in the *c8_location*\bin\fonts directory of the Cognos 8 server. If the Cognos 8 server is installed on a Windows computer, Cognos Report Studio also uses the fonts installed in the Windows font directory.

Changing the Language of the User Interface

In Cognos 8, the product locale controls the language of the user interface and all messages, including error messages. By default, the language you choose to run the installation program becomes the product language. Users can choose another language at run time.

The product locale is different from the content locale. The language in the user interface does not control the language or content of reports, or the object names, descriptions, or tips in Content Manager.

To change the language of the user interface, do the following:

- Determine which languages will be supported in the user interface
- Ensure that translations exist for all strings that appear in the Cognos 8 user interface, in the languages you require.
- Install language files on all computers in your distributed environment.
- Add or remove user interface language support using the Product Locale table on each Content Manager computer.

  By default, the user sees the product interface in the language that matches the language setting of the user locale.

  For more information, see the *Installation and Configuration Guide*.
- Map unsupported languages to supported languages using the Product Locale Mappings table on each Content Manager computer.

  You can then select the language to be used in the user interface when the language specified in the user locale is not available.

You can ensure that all regions for a locale use the same language, or that a specific, complete locale (language-region) uses a particular language.

Changing the Language of Reports, Data, or Metadata for Users

To ensure that users see reports, data, or metadata in their preferred language, or in a language specific to their region, add and remove partial locales (language) or complete locales (language-region) in the Content Locales table.

Adding incomplete locales (languages) to the Cognos 8 environment does not guarantee that your computer has a font that can show Web pages in your preferred languages. Ensure that you install the appropriate language packs to support the character sets you use. For more information, see "Adding Fonts to the Cognos 8 Environment" (p. 99).

Content locale consists of the language and region combinations that are supported for the following:

- Content Manager objects
- Framework Manager objects
- Content Manager data formatting
- report data formatting
- report text (titles)
- database data, if the database tool is configured to use locale

Content locale does not apply to PowerCubes, whether they are created in Cognos 8 Transformer or Cognos Series 7 Transformer. Each PowerCube is created with a single language encoding. For multiple languages, a separate PowerCube is required for each language.

If you have a multilingual model, you can specify the content locale of query data.

Users can create reports and access data using one of the supported languages, which include: English, French, German, Japanese, Dutch, Finnish, Swedish, Spanish, Italian, Portuguese, Traditional and Simplified Chinese, Korean, Czech, Hungarian, Polish, Romanian, Slovak, Greek, Turkish, Norwegian, Danish, and Russian.

The architecture is capable of supporting locales as well as additional languages. Therefore, it is possible to show data in two versions of English, each using a locale, such as en-us (English, United States) and en-ca (English, Canada).

User preferences allow the user to specify a locale or use the Web browser locale for both the product and content locale.

Mapping Content Locale

Some content is language-specific, such as names, and is called a partial locale. Some content is specific to language and region, such as date formats, and is called a complete locale. Use the Content Locale Mappings table to do the following:

- Ensure that users can access content that is language sensitive, but not locale sensitive.

  For example, map a complete locale, such as en-us (English, United States), to a partial locale, en, to ensure that users can access content in English that is not subject to regional variation. For example, names and descriptions are usually specified by language, not locale.

- Ensure that users can access content that is locale sensitive.

  For example, map a partial locale, such as en, to a complete locale, en-us, to ensure that users can access content that is locale sensitive, such as data format of dates and numbers. Data formatting is set by the combination of language and region and so requires a complete locale.

- Map a user-preferred language to another language.

  For example, a report is not available in the preferred language, Vietnamese, but is available in French and German. You can use the Content Locale Mappings table to map Vietnamese to French or German. You then see the report in the mapped language.

- Map unsupported content locales to supported locales.

When you map partial locales, Cognos 8 does the mapping after checking for a user locale. If all users are using the same Web browser types, mappings behave the same way for all users. However, if you have multiple browsers, results vary.

For example, on Internet Explorer, locale identifiers for many European regions do not exist. In other words, the user locale of fr-fr (French, France) cannot be selected. Only the fr (French language identifier) is available. To correct the problem, fr can be mapped to fr-fr, so that the language-region value is returned. Netscape provides region identifiers, so locale mapping is not required to return a value of fr-fr. This distinction may produce inconsistent results for different browser users. On Internet Explorer, where fr is mapped to fr-fr, users receive content that is region specific (fr-fr). On Netscape, where fr does not return a value of fr-fr, users receive content that is not region specific.

User Choices

In a Framework Manager model, users can specify the column titles and column descriptions that they want to see in their own language. A report automatically switches to the user preferred language. No action is required by the author.

In Report Studio, users can specify a language or locale for

- report data items, such as calculations, that do not exist in the metadata model
- text in a report, such as the page title
- report layouts

Customizing Currency, Numbers, Dates, and Times

Cognos 8 provides a complete set of default locale formats for number, dates (short, long, complete, and abbreviated), times, intervals, and currencies across almost 200 locales. You can control whether all formatting or a selected subset of data is linked to the user locale.

For example, data in US currency can be shown with the US currency symbol ($) and the format that is appropriate for the user locale. A French user may see 123,45 $, and a US user $123.45.

By default, Cognos 8 shows only a subset of supported currencies in the user interface. You add or remove currencies in the Currency table on each Content Manager computer.

When users are prompted for numerical data, Cognos 8 automatically accepts the data in the user locale format.

Support for Japanese Users

Dates in an Imperial calendar are entered and shown using the year, which can be specified as a year or a given emperor's reign.

Users have the option of using English year and month names for either the Imperial or Gregorian calendar.

Cognos 8 supports Sankaku negative signs. A triangle is used in place of the western negative sign (-).

Symbol	Shift-JIS	Unicode
△	0x81A2	U+25B3
▲	0x81A3	U+25B2
▽	0x81A4	U+25BD
▼	0x81A5	U+25BC

Setting up a Multilingual Cognos 8 Environment

You can create reports that show data in more than one language and use different regional settings. This means that you can create a single report that can be used by report consumers anywhere in the world.

You can combine data sources from multiple locales. If you use a Cognos Series 7 PowerCube as a data source, Cognos 8 converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube. After conversion in Cognos 8, PowerCubes from multiple locales can be combined with no concern about server locale.

The samples databases provided with Cognos 8 store a selection of text fields, such as names and descriptions, in more than 25 languages to demonstrate a multilingual reporting environment. For information about how data is stored in the samples databases and how the samples databases are set up to use multilingual data, see the *Administration and Security Guide*.

Here is the process for creating a multilingual reporting environment:

- Use multilingual metadata.

  The data source administrator can store multilingual data in either individual tables, rows, or columns.

  For more information about configuring your database for multilingual reporting, see the *Administration and Security Guide*.

- Create a multilingual model.

  Modelers use Framework Manager to add multilingual metadata to the model from any data source type except OLAP. They add multilingual metadata by defining which languages the model supports, translating text strings in the model for things such as object names and descriptions, and defining which languages are exported in each package. If the data source contains multilingual data, modelers can define queries that retrieve data in the default language for the report user.

  For more information, see the Framework Manager *User Guide*.

- Create multilingual maps.

  Administrators and modelers use a Windows utility named Map Manager to import maps and update labels for maps in Report Studio. For map features such as country and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

  For more information, see the Map Manager *User Guide*.

- Create a multilingual report.

  The report author uses Report Studio to create a report that can be viewed in different languages. For example, the report author can specify that text, such as the title, appears in German when the report is opened by a German user. Report authors can also add translations for text objects, and create other language-dependent objects.

  For more information, see the Report Studio *User Guide*.

- Specify the language in which a report is viewed.

  You can use Cognos Connection to do the following:

  - Define multilingual properties, such as a name, screen tip, and description, for each entry in the portal.
  - Specify the default language to be used when a report is run.

    Tip: You can specify the default language on the run options page, in the report properties, or in your preferences.
  - Specify a language, other than the default, to be used when a report is run.

    For more information, see the Cognos Connection *User Guide*.

The data then appears in the language and with the regional settings specified in

- the user's Web browser options
- the run options
- the Cognos Connection preferences

Any text that users or authors add appears in the language in which they typed it.

Configuring a Database for Multilingual Reporting

Cognos 8 is a Unicode product capable of querying and encoding data in many languages. Cognos 8 typically queries the database using the native data encoding of the database, such as Latin-1, Shift-JIS, and Unicode. Cognos 8 translates this data to Unicode as required.

When querying databases with two or more data encodings, Report Studio requests the data in Unicode. Some databases require specific configuration of the client or server software to enable this capability. For more information, see your database vendor documentation.

Round Trip Safety Configuration of Japanese Characters

Shift-JIS is the Japanese character encoding system. If characters are converted from Unicode to Shift-JIS and back to Unicode, round trip safety issues can arise. These can be avoided by using the Round Trip Safety Configuration utility. This utility is located in *c8_location*\bin and is named rtsconfig.exe.

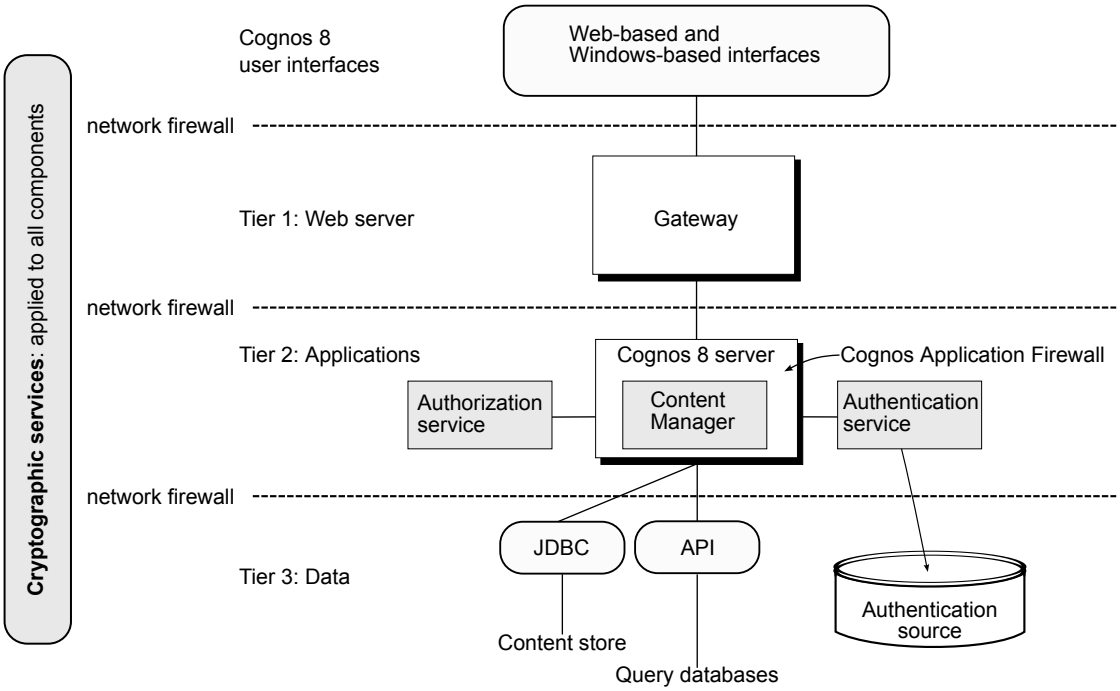
The Round Trip Safety Configuration utility ensures the round trip safety of Shift-JIS characters only when it is used to convert the characters both from Shift-JIS to Unicode and from Unicode to Shift-JIS. If data is requested from a database that has its own conversion mechanism to convert the Shift-JIS characters to Unicode automatically, Cognos 8 does not call the Round Trip Safety Configuration utility to convert the characters back to Shift-JIS. In this situation, the round trip safety of characters in the data cannot be ensured.

Chapter 10: Security Architecture

Cognos 8 provides a security architecture that is flexible and compatible with your existing security model. It is easily integrated with authentication and cryptographic providers.

Cognos 8 security involves the following:

- Cognos Application Firewall (p. 107)
- Cognos authentication services (p. 108)
- Cognos authorization services (p. 109)
- Cryptographic services (p. 110)



For information about setting up security in Cognos 8, see "Securing the Deployment" (p. 113).

Cognos Application Firewall

Cognos Application Firewall validates and filters incoming and outgoing traffic at the dispatcher layer.

Cognos Application Firewall features include request validation, SecureError, and parameter signing. It also has a flexible architecture that can be updated to keep your Cognos 8 security current.

Cognos Application Firewall is an essential component of Cognos 8 security, helping to provide protection against penetration vulnerabilities such as cross-site scripting. Disabling the Cognos

Application Firewall will remove this protection, and should not be done under normal circumstances (p. 119).

For information about configuring Cognos Application Firewall, see the *Installation and Configuration Guide*.

Cognos Authentication Services

Authentication is the process of identifying individuals before allowing them to log on.

Authentication in Cognos 8 is integrated with third-party authentication providers. Authentication providers define users, groups, and roles used for authentication. User names, IDs, passwords, regional settings, and personal preferences are some examples of information stored in the authentication source accessed by the provider. An authentication namespace is an instance of a configured authentication provider.

To set up authentication for Cognos 8, you must configure Cognos 8 using one or more of these authentication providers:

- LDAP
- Windows NT LAN Manager (NTLM)
- Microsoft Active Directory
- Cognos 7 namespaces created using Cognos 7 Access Manager and available with other Cognos products
- eTrust SiteMinder
- Custom Java provider

For information about configuring third-party authentication providers, see the *Installation and Configuration Guide*. For information about creating a custom authentication provider, see the Custom Authentication Provider *Developer Guide*, available when you purchase the Cognos 8 software development kit.

For information about anonymous access and authenticated access, see "Request Flow Processing" (p. 33).

Cognos Namespace

Cognos 8 has its own namespace that exists regardless of any additional namespaces that are configured based on third-party authentication providers. The Cognos namespace does not replicate the groups and roles defined in your authentication provider. Instead, you may want to use the Cognos namespace to define groups and roles that can span multiple third-party authentication providers. This practice can add value to your existing groups and roles by reorganizing them for Cognos 8 without changing them in your authentication provider.

You can use the Cognos namespace to set up security that links easily with client security systems. For an example, see "Using the Cognos Namespace to Restrict Access" (p. 123). For more information, see the *Administration and Security Guide*.

Single Signon

You can configure Cognos 8 for single signon. Users can then sign on once to an environment that includes Cognos 8 and other programs, without having to sign on each time they move between programs. Implementation of a single signon solution depends on the environment and authentication provider configuration.

For more information, see the *Installation and Configuration Guide*.

Cognos Authorization Services

Authorization is the process of granting or denying access to data, and specifying the actions that can be performed on that data, based on a user identity. For example, Cognos 8 administrators can set up folders in which reports are stored. They can then secure those folders so that only authorized users can view, change, or perform other tasks using the reports in the folder.

Authorization services are provided in Content Manager.

Distributed Administration

The Cognos 8 security model supports the distribution of security administration. Because objects in Content Manager, such as folders and groups, can be secured separately, security administration can be assigned to individuals in separate functional areas of the organization. Security administration does not have to be centralized with an Information Technology group or other overall administration group.

Permissions

Permissions define access rights to objects, such as directories, folders, and other content, for each user, group, or role. Permissions also define the activities that can be performed with these objects.

Cognos 8 authorization assigns permissions to

- groups and roles created in the Cognos namespace in Content Manager.

  These groups and roles are referred to as Cognos groups and Cognos roles.

- entire namespaces, users, groups, and roles created in third-party authentication providers.

Users

A user entry is created and maintained in a third-party authentication provider to uniquely identify an account belonging to a person or a computer. You cannot create user entries in Cognos 8.

The user entry stored in the authentication provider may include information such as first and last names, passwords, IDs, locales, and email addresses. However, Cognos 8 may require additional information, such as the location of the users' personal folders or their format preferences for viewing reports in the portal. This additional information is stored in Cognos 8.

You can assign users to groups and roles defined in the authentication provider and in Cognos 8. A user can belong to one or more groups or roles. If users are members of more than one group, their access permissions are merged.

For more information about users, see the *Administration and Security Guide*.

Groups and Roles

Groups and roles represent collections of users who perform similar functions, or have a similar status in an organization. Members of groups can be users and other groups. Members of roles can be users, groups, and other roles.

Both groups and roles are used to assign access permissions in Cognos 8. Users always log on with all the permissions associated with the groups and roles to which they belong.

For more information about groups and roles, see the *Administration and Security Guide*.

Cryptographic Services

Cryptographic services ensure that Cognos 8 communications and sensitive data are secure. Encryption is used to secure

- static data
- temporary data
- transient data

Two categories of encryption strength are available for Cognos 8. Basic encryption is the standard Cognos cryptographic service included with Cognos 8. If an assessment of your security risks indicates a need for stronger cryptographic services, you can replace the standard Cognos cryptographic services with one of the enhanced encryption modules.

For more information, see "Configuring the Cryptographic Environment" (p. 120).

Using a Third-party Certificate Authority

Cognos 8 relies on the functionality of a certificate authority (CA) to provide cryptographic services. By default, Cognos 8 provides a simple built-in CA. You may choose to disable it and use a third-party CA. You can use any third-party CA that generates Base-64 encoded X.509 certificates. For more information, see the *Installation and Configuration Guide*.

Standard Cryptographic Provider

The Cognos standard cryptographic provider, which uses Standard OpenSSL, is included with Cognos 8. It includes the following:

- secure sockets layer (SSL) services

  The SSL protocol is used to secure communication between Cognos 8 components installed on the same computer or on different computers.

- trusted requests on BI bus messages

  Signatures are used to digitally sign some messages to ensure that they come from a recognized Cognos 8 service.

- encryption of the deployment process

  Symmetric algorithms are used to encrypt and decrypt data in the export and import processes.

- encryption of temporary files

  Symmetric algorithms are used to encrypt and decrypt temporary files.

Data stored in the database depends on database security to protect it.

The standard Cognos cryptographic provider uses an encryption mechanism with keys up to 56 bits. Use it either with the built-in certificate authority (CA), or with a third-party CA.

Enhanced Cryptographic Providers

If you require stronger security, you can replace the standard Cognos cryptographic provider with a module that provides enhanced encryption.

Enhanced encryption modules are available from Cognos. They are packaged separately to adhere to government regulations controlling the export of cryptographic software.

You can add enhanced encryption after you start using Cognos 8 with standard encryption. However, after you install enhanced encryption and configure Cognos 8 to use it, you cannot return to standard encryption.

The Enhanced Encryption Module for OpenSSL

This module uses encryption algorithms with a key size up to 168 bits for symmetric encryption operations.

You can use the Enhanced Encryption Module for OpenSSL either with the built-in Cognos 8 certificate authority (CA) or with a supported third-party CA. To use a third-party CA, you must purchase and install appropriate software before you install and configure the Enhanced Encryption Module for OpenSSL.

The Enhanced Encryption Module for Entrust

This module uses encryption algorithms with a key size up to 168 bits for symmetric encryption operations.

If you choose the Enhanced Entrust encryption provider, you must purchase and install an Entrust Public Key Infrastructure (PKI), which includes its own CA. The PKI must be available before you install and configure the Enhanced Encryption Module for Entrust.

Chapter 11: Securing the Deployment

The primary goals of the Cognos 8 security strategy are

- to limit access to authorized data to the intended users
- to prevent modification of the data, or data presentation, by unauthorized users
- to prevent the theft or destruction of information
- to ensure that the application is available

You must ensure that users cannot, either through inadvertent or malicious actions, view data that they are not authorized to view, bypass authentication and authorization mechanisms, steal or violate session states to assume the identity of another user, or escalate existing privileges. You must also prevent users from causing disruptions in service for the application.

This information will help you configure a Cognos 8 installation for maximum security. The issues discussed include the environment security, which involves the operating system (p. 114) and network security (p. 118), and the application security (p. 119). All of these areas were considered during the security audit (p. 128) that was conducted on Cognos 8 as part of the developmental cycle.

Each customer's installation and configuration of Cognos 8 is unique. As a result, the security requirements for each installation and configuration are also unique. This section does not contain complete information about issues involved in securing a Cognos 8 environment. However, it provides guidelines and recommendations that supplement the more detailed information in the Cognos 8 *Installation and Configuration Guide*.

The Cognos 8 security framework is based on the industry standard approach to securing Web applications. This involves addressing security issues during the design and development of functional areas that are vulnerable to security threats.

The following Cognos 8 functional areas were developed with special attention to security.

Authentication and Authorization

User authentication and authorization prevent unauthorized users from accessing system components and data.

The effectiveness of the security strategy depends on the type of authentication and authorization.

Web Request and Content Validation

Web request and content validation checks the data before the data is processed.

The effectiveness of the security strategy depends on the validation techniques, such as bounds checking that prevents buffer overflow and variable assignment violations, and format checking that prevents data encoding and format string violations.

Session Management

Session management supports appropriate access control. It relies on strong session identifiers that are difficult to guess.

The effectiveness of the security strategy depends on the type of session management systems used, the information that they include, and where in the program cycle the sessions are validated.

Transport Security

Transport security is used during transmission to secure transactions that contain sensitive information when untrusted networks are used.

The effectiveness of the security strategy depends on how data is encrypted.

Encryption

Encryption protects sensitive data, such as account credentials and personal information.

The effectiveness of the security strategy depends on how data is encrypted and stored.

Logging and Monitoring

Application logs identify when errors occur or when sensitive transactions are complete. In addition, application logs record error messages that provide system information. Error messages should expose the minimum amount of information to meet business requirements.

The effectiveness of the security strategy depends on where the log files are stored, and whether auditing capabilities are built into the application.

Administration

Administrative access includes the right to add and remove users, provide group and role-based access, and configure application components. Administrative access should be restricted to appropriate individuals.

The effectiveness of the security strategy depends on how the application is administered, the configuration of administrative options for security, and how these options are protected.

Techniques for Securing the Operating System

The operating system is the physical environment where your application runs. Any vulnerability in the operating system could compromise the security of the application. By securing the operating system, you make the environment stable, control access to resources, and control external access to the environment.

The physical security of the system is essential. Threats can come through the Web, but they can also come from a physical terminal. Even if the Web access is very secure, if an attacker obtains physical access to a server, breaking into a system is much easier.

We strongly recommend that you review security policies and recommendations for your operating system. Consider implementing the following security best practices.

User Accounts

- Limit the number of user accounts on the server computers.

  Unnecessary and legacy user accounts increase system complexity and may present system vulnerabilities.

  Fewer user accounts reduces the amount of time administrators spend on account administration.

- Ensure that only a few trusted users have administrative access to the server computers.

  Fewer administrators make it easier to maintain accountability. The administrators must be competent.

- Assign the minimum required access permissions for the account that runs the application.

  If attackers obtain access to the application, they have the permissions of the user who runs the application.

Account Policies

- Develop and administer password policies that promote operating system security.

  Examples of such policies are the strong password rule and the password change schedule.

- Test the strength of users' passwords by breaking the passwords.

  The users who do not comply with the strong password rule receive a notification to update their passwords according to the organization password policy.

  Software is available to help you with this task.

- On UNIX, activate the shadow password file.

  On UNIX, passwords are stored in the /etc/passwd file. This file is open to everyone, which presents a security risk. To enhance password security, activate the shadow password file named /etc/shadow. If this file is available, passwords are stored in it instead of the passwd file. Because permissions for the /etc/shadow file are more restrictive, the security risk is lower.

File System

- Grant the users read-only permissions for required directories.

  If attackers obtain access to an application, they have the user permissions.

- Deny access by default.

  Access to resources is denied for everyone except for the users to whom access is granted explicitly.

  You can deny read and write permissions for all directory structures for all users. Only users to whom these permissions are granted explicitly have access to the directories and files. This policy also protects any resources that were overlooked by an administrator.

Network Services

- Provide the minimum number of required services on the server computer.

Use only the services that you need to run the application. Each service is a potential entry point for a malicious attack. Reducing the number of running services also makes your system more manageable.

For example, you may not need the ftp, rlogin, or ssh services.

- Reduce the level of access permissions for the network services users.

  Network services are exposed to the public.

- Ensure that the user accounts that have access to the Web server do not have access to the shell functions.

- Ensure that unused services do not exist in the rc files, rc0 through to rc6, in the /etc directory on UNIX and Linux.

- Ensure that unused services are not running, and that they do not start automatically on Windows.

- Ensure that required services are running on UNIX.

  You can use the ps and netstat utilities to see the running services. The ps utility gives a list of processes currently running on the computer. The netstat utility provides a list of ports that are currently in use.

- Reduce the number of trusted ports specified in the /etc/services file.

  Delete or comment out the ports that you do not plan to use to eliminate possible entry points to the system.

- Protect your system against NetBIOS threats associated with ports 137, 138, and 139.

  These ports are listed in the /etc/services file.

- Use wrapper services, such as iptables.

- Ensure that the services are current by checking often for security updates.

- Avoid using services that have a graphical user interface (GUI), if possible.

  Such services introduce many known security vulnerabilities.

System Patches

- Run the latest, vendor-recommended patches for the operating system.

  The patches may be core OS patches, or patches required by additional applications.

- Schedule regular maintenance of security patches.

Operating System Minimization

- Remove nonessential applications to reduce possible system vulnerabilities.

- Restrict local services to the services required for operation.

- Implement protection for buffer overflow.

You may need third-party software to do this.

Logging and Monitoring

- ❑ Log security-related events, including successful and failed logons, logoffs, and changes to user permissions.
- ❑ Monitor system log files.
- ❑ Use a time server to correlate time for forensics.
- ❑ Secure the system log files by restricting access permissions to them.

  Logs are important for daily maintenance and as a disaster recovery tool. Therefore, they must be protected from system failures and user tampering.
- ❑ Use IPF logging to build a more sophisticated logging system.

  To increase the security of the log file system, you can

  - place all log files in one location, on one server

    This simplifies the administration of log files.
  - set up multiple logging servers for redundancy
  - use a remote server for logging

    This protects the logs if the system is compromised and, for example, the hard drive is destroyed.

    Because an IPF server is accessed through the network, it can be located anywhere in the world.
- ❑ Secure the logging configuration file.

  The configuration file contains settings that, if changed, can compromise the reliability of the log system. For example, setting the log level incorrectly may cause some failures not to be logged.
- ❑ Enable logging of access requests on the Web server.

  This can be useful in identifying malicious activity.

System Integrity

- ❑ Build production systems from a known and repeatable process to ensure the system integrity.
- ❑ Check systems periodically against snapshots of the original system.
- ❑ Use available third-party auditing software to check the system integrity.
- ❑ Back up the system resources on a regular basis.

Techniques for Securing the Network

The network is the entry point to an application. Therefore, the network security mechanisms are the first line of defense against potential threats from the outside. Network security involves protecting the protocols and the communication channels, as well as devices, such as the router, the firewall, and the switch.

Consider implementing the following best practices to enhance your network security:

- Use a firewall.

  This will allow only legitimate access to the network.

- Ensure that the firewall provides packet forwarding and filtering.

  These firewall features introduce an additional layer of protection. Forwarding packets prevents the outside world from direct contact with the computers inside the protected network. Filtering can block some types of requests, or requests that come from some domains or IP addresses. These techniques help to reduce the number of illegitimate requests that can be passed to the internal network.

- Limit the number of accessible ports.
- Limit the traffic direction on some ports.
- Limit some network protocols, such as ping.

Web Servers

Consider implementing the following security best practices for all types of Web servers:

- Remove any unused virtual directories.
- Grant read, write, and execute permissions explicitly for each Web site and virtual directory.
- Create a root directory for the Web server.

  For Apache, this is known as chrooting.

  For IIS, you can assign the root Web site to a specific directory. The user who runs IIS can be given read and write permissions for this directory. All other user permissions can be removed.

- Ensure that access permissions for the physical files are set up properly.

  Only some users require read and write permissions for these files.

- Remove unwanted default mappings, such as for applications with the .htr, .idc, .stm, .printer, and .htw file extensions.
- Enable secure sockets layer (SSL) on the Web server.

  SSL is used to encrypt a user's communication with the Web server. For more information, see the section about configuring the Web server in the *Installation and Configuration Guide*.

For Apache, also implement the following best practices:

- Enable only the required modules.

- Ensure that your Apache installation hides version information and other sensitive information.
- Turn off directory browsing.
- Configure the Web server to restrict access by IP address.
- Ensure that error logging and access logging are enabled.

  These types of logging are controlled by the ErrorLog and mod_log directives in the configuration file.

For IIS, also implement the following best practices:

- Disable protocols, such as ftp, if they are not used.
- Enable logging in the configuration tool.
- Disable Remote Data Service if it is not required.
- Remove sample applications, such as \\IISSamples, \IISHelp, and \MSADC.
- Set access permissions for the `winreg` registry key.

  Only administrators require access to this key.

Securing the Application

Using the built-in security features, you can configure a Cognos 8 installation for maximum security.

The best practices provided here are not a complete list of all configuration tasks required to secure your application. However, they address the most critical issues that include Cognos Application Firewall (p. 119), the cryptographic environment (p. 120), the SSL protocol (p. 121), and the temporary files (p. 122). They also address securing access to Cognos Connection (p. 123), Cognos PowerCubes (p. 127), data source signons (p. 127), and the content store (p. 128).

Recommendation - Use Cognos Application Firewall

Cognos Application Firewall (CAF) supplements the existing Cognos 8 security infrastructure. By default, this supplemental security is enabled. To ensure that the Cognos 8 solution is secure, CAF should never be disabled in a production environment.

In a distributed environment, all CAF settings must be the same for all computers where Cognos 8 Application Tier Components are installed. If CAF is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

CAF protects the Cognos 8 components from processing malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting attacks (XSS links), either through script injection in valid pages or redirection to other Web sites.

Using Cognos Configuration, you can change settings for third-party XSS tool support, and add host and domain names to the Cognos list of valid names.

You can also track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the *c8_location*\logs\cogserver.log file.

Configuring the Cryptographic Environment

We recommend that you assess the level of security required for your environment before setting up the system. Typical factors that influence the decision how secure a system must be, include

- external exposure

  Who are the users? Are there internal users as well as external or guest users?

- use of the public Internet

  Is the system accessible by the Internet? Does a virtual private network (VPN) exist?

- data sensitivity

  Departments such as human resources, finance, and accounting likely want the data protected the best way possible.

For more information about cryptography in Cognos 8, see "Cryptographic Services" (p. 110). For more information about configuring the cryptographic settings, see the *Installation and Configuration Guide*.

Cryptographic Providers and Cipher Strength

Cognos 8 components require a cryptographic provider to run (p. 110). If you delete the default cryptographic provider, you must configure another provider (p. 111).

The default cryptographic provider uses keys up to 56 bits for data encryption and secure sockets layer (SSL) protocol. If your organization needs stronger encryption, you can configure enhanced cryptographic providers that use key sizes greater than 56 bits, such as the Enhanced Encryption Module for OpenSSL or the Enhanced Encryption Module for Entrust. Both providers are available from Cognos.

When choosing the cryptographic provider, cipher strength should not be the main concern. The encryption provided by the standard Cognos provider is secure enough for most applications. A high-security setup relies not only on the cipher strength, but on the security of the whole system, which includes physical access to directories, password policies, and so on. Only if your environment is exposed to the Internet and deals with highly sensitive data, you should consider using the enhanced encryption modules.

The Certificate Authority (CA)

When you implement the standard or enhanced Cognos cryptographic provider (p. 110), the Cognos 8 certificate authority, AutoCA, is used by default. AutoCA signs the internal certificates and provides all the functionality needed to establish the root of trust in the Cognos security infrastructure.

AutoCA is sufficient for simple setups and test environments, but has limitations in development and production environments. For example, it cannot provide full administration capabilities for issued and revoked certificates, issue certificates based on purpose, such as mail, server, and private certificates, or sign the Web server and client certificates.

If you intend to enable SSL for the Web server or application server, or use client certificates, you need a third-party CA. This can likely be a CA that your organization already implemented as part of its security infrastructure. When using a third party CA, the necessary certificates must be

generated and imported. For more information, see the section about configuring Cognos 8 components to use a third-party certificate authority in the *Installation and Configuration* Guide.

For internal systems that are not exposed to the Internet, you can set up your own CA using the open source software OpenSSL.

Cognos 8 does not support self-signed certificates because they do not adhere to the public key infrastructure (PKI) principles.

Supported Cipher Suites and Application Servers

In distributed installations, you must specify the same set of cipher suites for all installation components. Mixing ciphers, especially weak and strong, can cause problems. The sets must contain at least one common suite. Otherwise, the SSL negotiation fails and the connection cannot be established.

The cipher suites are also affected by the application server that is used to run Cognos 8. If Tomcat is used, the Cognos code generates the server certificates and switches Tomcat to SSL listeners. The cipher suites configured in Cognos 8 are the only ciphers that can be used. If an application server other than Tomcat is used, SSL must be enabled on the application server before the cipher suites are configured in Cognos 8. Ensure that the set of cipher suites you specify in Cognos Configuration contains at least one of the cipher suites configured on the application server. Otherwise, the SSL connection will not initialize.

Specify the list of cipher suites in priority sequence where the stronger ciphers appear first.

The following cipher suites are supported for deployments that use standard or enhanced encryption:

- RSA-RSA-DES(56)-CBC-SHA
- DH-RSA-DES(56)CBC-SHA
- RSA-RSA-RC4(40)-MD5
- RSA-RSA-DES(40)-SHA
- DH-RSA-DES(40)-SHA
- DH-None-DES(40)CBC-SHA

Additionally, for deployments that use enhanced encryption, cipher suites with keys greater than 56 bits are supported.

Enabling SSL

When you use secure sockets layer (SSL), you protect the data crossing between the Web servers, application servers, and LDAP servers. Except for the Web servers, the servers are internal and protected by a firewall. You can usually rely on the network security for external network links. If this security is not enough, SSL should be enabled for communications between Cognos 8 components and other servers.

Enabling SSL requires a certificate authority (CA) (p. 120), and an administrator with a good knowledge of the public key infrastructure (PKI) technology and SSL.

You can configure Cognos components to use the SSL protocol for

- internal connections

  If you configure SSL only for internal connections, Cognos components on the local computer communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, HTTP requests. Therefore, you must configure two dispatcher URIs.

  If you use Tomcat to run Cognos 8, you configure the SSL protocol in Cognos Configuration. If you use a different type of application server, the SSL protocol must be configured on the application server.

- external connections

  If you configure SSL only for external connections, communications from remote Cognos components to the local computer use the SSL protocol. You must configure the dispatcher to listen for secure remote requests on a different port than local HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

  For externally accessible Web servers, SSL should always be enabled. For more information, see the *Installation and Configuration Guide*

- internal and external connections

  If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

  You must also update the Content Manager URIs, dispatcher URI for external applications, and Gateway URI to use SSL, if required.

- LDAP connections

  If you use an LDAP directory server, you can enable LDAPS, the secure LDAP protocol, for communications between the Access Manager component of Content Manager and the LDAP directory server. Unsecured LDAP traffic is transmitted as clear text.

  To enable LDAPS, you must install a server certificate that is signed by a certificate authority (CA) in your directory server, create a certificate database to contain the certificates, and configure the directory server and the Cognos 8 LDAP namespace to use LDAPS.

  For more information, see the sections about configuring LDAP authentication providers in the *Installation and Configuration Guide*.

For more information about configuring the SSL protocol, see the *Installation and Configuration Guide*.

Securing Temporary Files

Cognos 8 uses temporary files during reporting activities to store recently viewed reports. The files are not encrypted. Because the reports can contain sensitive data, they should be secured.

We recommend that you implement the following measures:

- Restrict access to the temporary files directory.

Grant read and write permissions for the temp directory only to the Cognos 8 service account. Deny all other accounts any access.

The temp directory can be in the default *c8_location*\temp location, or in a different location, as specified in Cognos Configuration.

- Enable encryption of temporary files.

  Because encrypted content is unintelligible, it is useless for potential attackers.

  Encrypting temporary files may affect performance.

For more information, see the section about configuring temporary files properties in the *Installation and Configuration Guide*.

Techniques for Securing Access to Cognos Connection

When you add an authentication provider in Cognos Configuration, all users in the directory have access to Cognos Connection. To secure Cognos 8, you must restrict this access.

The methods and best practices discussed in this section apply mostly to the LDAP authentication providers, Sun Java System directory server and Active Directory.

Use whichever of the following methods applies to your organization:

- the Cognos namespace (p. 123)

  Use this method with any type of authentication provider when you want to grant access only to the members of the Cognos namespace.

- LDAP groups or roles (p. 124)

  Use this method with Sun Java System directory server or Active Directory when the user accounts are located in different branches of the directory tree.

- LDAP OUs (p. 126)

  Use this method with Sun Java System directory server or Active Directory when the user accounts are located in a specific Organizational Unit (OU) in the directory tree.

  An Organizational Unit (OU) is a type of container in an LDAP directory structure. OU can contain user accounts, groups, roles, and other OUs.

Using the Cognos Namespace to Restrict Access

You can restrict access to Cognos Connection only to users who belong to any group or role defined in the Cognos namespace. This is a quick method of securing access to Cognos Connection that can be used with any type of authentication provider. Several built-in groups and roles in the Cognos namespace can be used. You can also create new groups and roles.

Tip: In Cognos Configuration, set the value of the **Restrict access to members of the built-in namespace** property to **True**.

Before you use this method, you must

- ensure that authorized users and groups belong to at least one Cognos group or role

Add the user accounts, groups, and roles created in your authentication provider to the Cognos namespace.

- remove the group Everyone from the built-in and predefined Cognos groups and roles

  By default, the group Everyone is a member of all built-in and predefined groups and roles in the Cognos namespace.

For more information about managing groups and roles in Cognos 8, see the *Administration and Security Guide*. For more information about configuring Cognos 8 to use an authentication provider, see the *Installation and Configuration Guide*.

Using LDAP Groups or Roles to Restrict Access

Not all users in your LDAP directory must use Cognos 8. Grant only designated users access to Cognos Connection. This can be done by creating a Cognos 8-specific group or role in your directory server, adding the required users to its membership, and granting the group or role access to Cognos Connection.

An alternative method is based on using the LDAP organizational units (OUs) (p. 126).

Whether you must create a group or a role depends on your authentication provider. If you use Sun Java System directory server, you must create roles because this provider uses role membership as part of its user account information. If you use Active Directory, you must create groups because this provider uses group membership as part of its user account information.

Using Roles

The roles for this technique are created using Sun Java System directory server. For more information about creating this type of roles, see the Sun Java System documentation.

Ensure that the following parameters are properly defined in Cognos Configuration, in the **Security**, **Authentication** category.

- **User lookup**

  Configure the user lookup string to contain the attribute that will be used to authenticate against the `${userID}` variable. This variable takes the user name entered at logon and substitutes the variable with the value before passing the search string to the directory server. The distinguished name (DN) of the role must also be included in the string.

  Here is an example of the lookup string: `(&(uid=${userID})(nsrole=cn=Cognos8,ou=people,dc=cognos,dc=com))`

  In this example, all members of the Cognos 8 role located in the organizational unit (ou) named people have access to Cognos Connection.

- **Use external identity?**

  Set the value to **True** if single signon is enabled.

- **External identity mapping**

  Specify this property if **Use external identity?** is set to **True**.

Construct a string to locate a user in the LDAP directory server. At logon time, the environment variable `${environment("REMOTE_USER")}` in this string is replaced by the user name.

In the following example, the Web browser sets the environment variable `REMOTE_USER` that matches the user's `uid` attribute:

```
(&(uid=${environment("REMOTE_USER")})
(nsrole=cn=Cognos8,ou=people,dc=cognos,dc=com)).
```

In some cases, the `REMOTE_USER` variable, which is typically in the DOMAIN\username format, may not match any of the user's `uid` attributes. To solve this problem, include the `replace` function in the string, as in the following example:

```
(&(uid=${replace(${environment("REMOTE_USER")},"ABC\\","")})
(nsrole=cn=Cognos8,ou=people,dc=cognos,dc=com))
```

If the `replace` function is included, the domain name, ABC in this example, is replaced with a blank string, and only the user name is passed to the directory server.

The domain name is case sensitive in this context.

After the role is created, configure it for access to Cognos Connection using Cognos Configuration. The role can also be added to the Cognos namespace.

Using Groups

The groups for this technique are created using Active Directory. This technique involves modifications to the user lookup string. Because Active Directory does not have this property, it cannot be used. Instead, the associated LDAP provider is used.

Ensure that the following parameters are properly specified in Cognos Configuration, in the **Security**, **Authentication** category.

- **User lookup**

  Configure the lookup string to contain the attribute that will be used to authenticate against the `${userID}` variable. This variable takes the user name entered at logon and substitutes the variable with the value before passing the search string to the directory server. The distinguished name (DN) of the group must also be included in the string.

  Here is an example of the lookup string: `(&(sAMAccountName=${userID})
(memberOf=cn=ReportNet,ou=Groups,dc=cognos,dc=com))`

- **Use external identity?**

  Set the value to **True** if single signon is enabled.

- **External identity mapping**

  Specify this property if **Use external identity?** is set to **True**.

  Construct a string to locate a user in the LDAP directory server. At logon time, the environment variable `${environment("REMOTE_USER")}` in this string is replaced by the user name and then the string is passed to the directory server.

In the following example, the Web browser sets the environment variable `REMOTE_USER` that matches the user's `uid` attribute. Instead of substituting the hard-coded `sAMAccountName` value with `${userID}`, the environment variable is read from the browser session.

```
(&(sAMAccountName=${environment("REMOTE_USER")})
(memberOf=cn=Cognos8,cn=Groups,dc=cognos,dc=com))
```

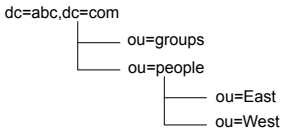
After the group is created, configure it for access to Cognos Connection using Cognos Configuration. The group can also be added to the Cognos namespace.

Using LDAP OUs to Restrict Access

You can grant access to Cognos Connection for a particular Organizational Unit (OU) or children of a particular OU in an LDAP directory. An OU usually represents a segment of an organization.

For this method to work, you must properly set up the **Base Distinguished Name** and **User lookup** properties in Cognos Configuration, under the **Security**, **Authentication** category. By using different values for these properties, you can grant access for different OUs in your LDAP directory structure.

Consider the following directory tree:



If users from only the East OU need access to Cognos Connection, the values can be specified as follows.

Property	Value
Base Distinguished Name	ou=East, ou=people, dc=abc, dc=com
User lookup	uid=${userID}

If users from both East and West OUs require access, the values can be specified as follows.

Property	Value
Base Distinguished Name	ou=people, dc=abc, dc=com
User lookup	(uid=${userID})

The parentheses () in the **User lookup** property are used as a filter that can search all OUs located under the specified Base DN. In the first example, only the East OU is searched for user accounts. In the second example, both the East and West OUs are searched.

However, in both of the above examples, groups are excluded from access to Cognos Connection because they are located in a different branch of the directory tree than users. To include both the

groups and users, the Base DN must be the root of the directory tree. The values would then be as follows.

Property	Value
Base Distinguished Name	dc=abc, dc=com
User lookup	(uid=${userID})

As a result, all users in the directory have access to Cognos Connection.

The last example shows that using OUs may not always be the most efficient way of securing access to Cognos Connection. You can use this method if you want to grant access for all users in a particular OU. If you want to grant access only for specific users, you may want to consider creating a designated Cognos 8 group or role in your directory server, and granting this group or role access to Cognos Connection (p. 124).

Securing Cognos PowerCubes

Cognos Series 7 PowerCubes are secured using the user class views based on the user classes that exist in the Series 7 namespace. After the PowerCubes are deployed into Cognos 8, the MDC files continue to reside in the file system.

As an additional security measure, we recommend that you

- set up restricted access to PowerCube data sources
- use a third-party file encryption system for the PowerCube data sources
- set up permissions for the Cognos 8 directory that contains the cubes
- grant read and write permissions for the users who must add or remove cubes from the directory
- grant read permissions for the domain user account that is used to start the Cognos 8 service

To use secured PowerCubes from Cognos Series 7 in Cognos 8, you must have a Series 7 namespace configured as an available authentication provider. PowerCubes that you create in Cognos 8 can be secured against any available authentication provider.

For more information, see the Transformer *User Guide* or the *Administration and Security Guide*.

Securing Data Source Signons

Cognos 8 uses data source signons to access the underlying data located in the reporting databases.

To protect against unwanted access to the data, we recommend that you

- grant execute permissions for users and groups that need the signons

  Other types of permissions are not required.
- deny execute permissions explicitly for all users, groups, and roles that do not need the signons

  This ensures that access is not permitted through an unknown membership.

For more information about data source signons, see the *Administration and Security Guide*.

Securing the Content Store

To ensure its security and integrity, the content store is accessed by the Content Manager service using single database signon specified in Cognos Configuration. The database signon is encrypted according to your encryption standards. However, the content store security relies not only on the Cognos 8 security but also on the native database security, operating system security, and network security.

For securing your database, we recommend that you follow these guidelines:

- Secure the database and the database API using the mechanisms provided by the database, the network, and the operating system.
- Assign a limited number of users to maintain the database.
- Use your database native security to grant only minimum permissions to the user accounts that access the database, as follows:
  - MS SQL Server

    Users must have create and drop table permissions for the database. Ensure that the user account is a member of the db_ddladmin, db_datareader, and db_datawriter roles, and the owner of their default schema.
  - ORACLE

    Users must have permissions to connect to the database. Also, they must be able to create, alter, and drop tables, triggers, views, procedures, and sequences, as well as insert, update, and delete data in the database tables. The permissions must be granted to the user account directly, and not through a group or role membership.
  - DB2

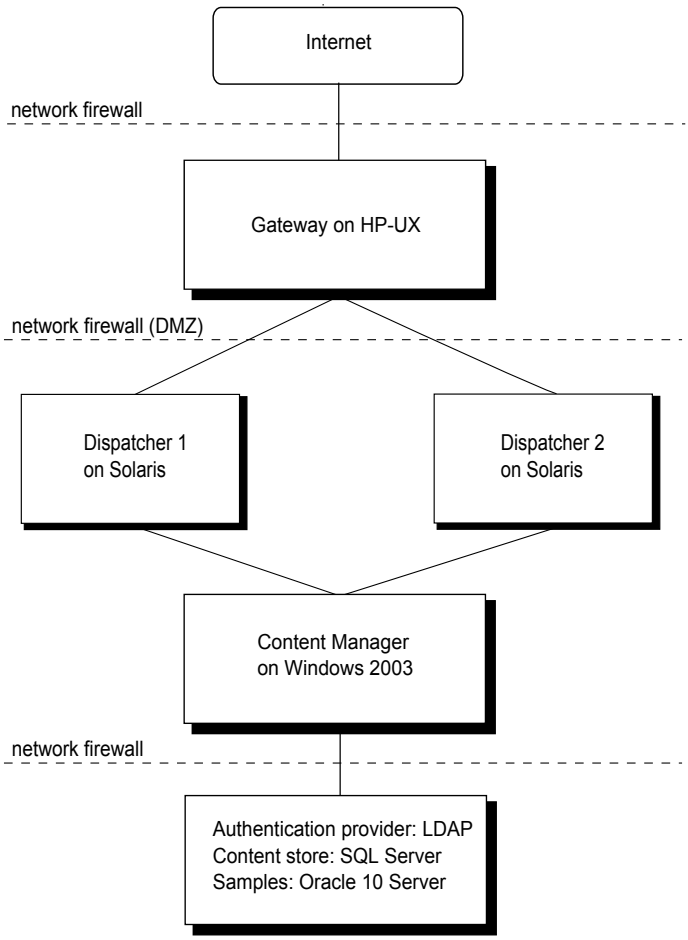
    Users must have the create, drop table, CREATETAB, CONNECT and IMPLICITSCHEMA permissions for the database. Also, they must have USE permissions for the USER TEMPORARY tablespace and other appropriate tablespaces associated with the database.
  - Sybase Adaptive Server Enterprise

    Users must have create, drop table, create default, create procedure, create rule, create table, and create view permissions for the database.
- Limit the number of users who have read or write access for the Content Manager tables.
- Follow other recommendations on securing the database provided by the database vendor.

Security Audit

A methodical security audit was conducted on Cognos 8 to check the effectiveness of the implemented security strategy.

The following distributed installation was used during the audit.



Index

Symbols

.xml configuration files, 45

A

absolute affinity, 79
accessing Cognos 8, 34
    anonymous access, 34
    authenticated access, 35
Access Manager, 24
Active Directory, 123
ActiveX, 14
administration, 47
    Cognos Connection, 47
    distributed, 109
affinity
    Cognos 8 activities, 91
    high, 90
    low, 91
    request, 78
    setting, 90
agents
    running, 40
agent service, 20
analysis
    Analysis Studio, 16
    running, 36, 38
    viewing, 36
Analysis Studio, 16
Apache Tomcat, 82
    memory settings, 87
Apache Web server, 118
application servers
    SSL, 121
    tuning, 87
applications tier, 19
Application Tier Components, 19
    installing, 58
    log server, 28
Architect models
    migration to Cognos 8, 65
architecture
    communications, 27
    scalability, 75
    security, 107
    workflow, 43
audience of document, 7
audit logs
    log destinations, 28
    See Also log messages
    See Also troubleshooting
authenticated access, 35
authentication, 108
authentication providers
    Active Directory, 123
    Series 7 namespace, 127
    Sun Java System, 123
authorization services, 109
author locale, 98
availability, 69
    Cognos 8 gateway, 81
    Cognos 8 server, 82
    Content Manager, 82
    content store, 83
    maximizing, 81
    planning, 81

B

balancing loads, 28
batch report service, 20
batch report services
    tuning, 90
best practices
    security, 113
BI Bus API, *See* Cognos 8 BI Bus API
browsers
    configuring, 46, 99
    fonts in HTML reports, 99

builds
running in Cognos Connection by using Data Movement service, 67
bursting reports, 93

C

capacity planning, 69
infrastructure components, 72
certificate authority, 110, 120
CGI, *See* common gateway interface
cipher strength, 120
cipher suites, 121
coglocale.xml files, 45
Cognos 8
accessing, 34
communications, 27
configuring, 45
dispatchers, 22
gateways, 18
installing, 44
performance tuning, 85
scalability, 75
security, 107, 110
services, 22
tuning, 89
user interfaces, 13
workflow, 43
Cognos 8 BI Bus API, 27
Cognos 8 Go! Office, 17, 32, 50
Cognos 8 Go! Search
using to search Cognos 8 BI content, 67
Cognos 8 servers, 19
availability, 82
monitoring, 95
Cognos 8 services
scalability, 80
Cognos Administration, 15
Cognos Application Firewall, 19, 107, 119
Cognos BI Bus API, 27
Cognos Configuration, 45
user interfaces, 13
Cognos Connection, 14
opening a folder, 39
securing, 123, 124, 126
Cognos Content Database, 24, 25
Cognos Controller
data access in Cognos 8, 66
Cognos DecisionStream
requirements to upgrade catalogs to Cognos 8, 64
Cognos Finance
data access in Cognos 8, 66
Cognos Go! Mobile
mobile reports, 67
Cognos Metrics Manager
requirements to upgrade to Cognos 8, 64
upgrading to Cognos 8, 63
Cognos namespace, 46, 108
securing Cognos Connection, 123
Cognos NoticeCast
duplication of functionality in Cognos 8, 68
Cognos Planning - Analyst
data access in Cognos 8, 65
Cognos Planning - Contributor
data access in Cognos 8, 65
migration to Cognos 8, 65
Cognos Portal Services
migration overview, 68
Cognos PowerPlay Web
requirements to upgrade reports to Cognos 8, 64
Cognos Query
duplication of functionality in Cognos 8, 67
Cognos Report Studio, 49
CognosScript
migration overview, 68
Cognos Series 7
migration to Cognos 8, 64
Cognos Series 7 PowerCubes
requirements for successful language conversion, 66
Cognos Visualizer
duplication of functionality in Cognos 8, 68
Cognos Web Services
migration overview, 68
cogstartup.xml files, 45
common gateway interface, 18
common symmetric key, 82
in encryption, 110
communications, 27
components
Cognos 8, 55
installing, 55
startup configuration, 45

Composite Information Server, 25
compressing PDF reports, 24
configuration
  browsers, 99
  fonts, 99
  multi-lingual reporting, 46
  planning, 53
  security, 46
  startup, 45
  Web browsers, 46
configuration files, 45
connecting to database, 31
connection limits
  setting, 87
connections
  low bandwidth, 95
content locale, 98
content locales, 101
  mapping, 102
Content Manager, 19, 22
  availability, 82
  installing, 58
  log server, 28
  scalability, 80
  standby, 19, 80
Content Manager service, 20
content providers, 24
content store, 24
  availability, 83
  securing, 128
  sizing, 73
control affinity, 79
cookies
  browser settings, 99
copyright material
  printing, 9
creating
  models, 48
  packages, 48
  reports, 49
cryptographic keys
  common symmetric key, 110
  encryption key pair, 110
  signing key pair, 110
cryptographic providers, 120
  cipher strength, 120
  enhanced, 111
  standard, 110
cryptographic services, 110
cryptography
  configuring, 120
CSK, *See* common symmetric key
currency, 103

D

data
  data sources, 24
  multilingual, 104
database
  configuring for multilingual reporting, 105
  modeling, 48, 50
  tuning, 87
database connection management, 31
  content store database, 31
  metric store databases, 32
  query databases, 32
data integration service, 20
Data Manager
  using in Cognos 8 BI, 67
Data Movement service
  using in Cognos Connection, 67
data source signons
  securing, 127
data tier, 24
dates, 103
DecisionStream
  requirements to upgrade catalogs to Cognos 8, 64
DecisionStream to Cognos 8
  upgrade consideration, 63
default settings
  browsers, 99
  fonts, 99
  security disabled, 107
delivery service, 20
diagnostics, *See* troubleshooting
disk maintenance, 95
dispatcher metrics, 85
dispatchers, 19
  load balancing, 76
  logging, 107
  tuning, 89

dispatching, 28
    local preferred, 28
distributed administration, 109
distributing
    requests, 28

E

enabling SSL, 121
encryption
    enhanced module for Entrust, 111
    enhanced module for Open SSL, 111
    key pairs, 110
    key size, 111
    strong, 111
Enterprise Information Integrators, 26
Entrust enhanced encryption module, 111
event management service, 20
Event Studio, 16
Excel, *See* Microsoft Office

F

finding information, 8
firewalls, 19, 107
    Framework Manager installation, 62
fonts
    configuration, 99
    installing, 46
formats
    numbers, 103
Framework Manager, 17
    configuration requirements, 61
    installation options, 61
    modeling, 48, 50
    packages, 48

G

gateways
    Cognos 8, 18, 56
    installing, 56
    scalability, 75
Global Customer Services Web site, 9
globalization considerations, 97
groups, 110
    securing Cognos Connection, 124

H

help
    getting, 9
high affinity, 79
HTML reports
    running, 36, 37
    viewing, 36

I

IBM WebSphere Portal, 14
IIS Web server, 118
implementation planning, 44
    checklist, 53
Impromptu catalogs and reports
    migration to Cognos 8, 65
Impromptu Web Reports
    migration to Cognos 8, 65
information
    finding, 8
installation
    Application Tier Components, 58
    components, 44
    Content Manager, 58
    fonts, 46
    Framework Manager, 61
    gateways, 56
    Metric Designer, 61
    options, 55
    planning, 53
    setting up security, 110
interfaces, 13
Internet Server API, 18
ISAPI, *See* Internet Server API

J

job service, 20
JobStreams
    running in Cognos Connection by using Data Movement service, 67
JVM metrics, 85

L

language
    restrictions for PowerCubes, 101

languages
supported, 101
user interface, 100
user preferences, 101
LDAP
namespaces, 123
load balancing, 75
automatic in Cognos 8, 76
configuring, 76
settings, 28
with external mechanisms, 77
without external mechanisms, 76
load distribution
application complexity, 72
concurrent users, 70
estimating, 71
locales
author, 98
content, 98, 101
content mapping, 102
description, 98
product, 98, 100
run, 99
server, 98
user, 98, 99
local preferred dispatching, 28
log destinations
types of, 28
logging
dispatcher, 107
secure, 107
logging database
adding metrics, 85
log messages
log destinations, 28
remote log server, 28
See Also audit logs
See Also troubleshooting
logs
message processing, 28
service, 21
low affinity, 79

M

maintaining disks, 95
Map Manager, 18, 104
maximizing availability, 81
memory settings
Apache Tomcat, 87
messaging, 28
metadata modeling, 48, 50
Metric Designer, 17
configuration requirements, 61
installation options, 61
metrics, performance, 85
Metrics Manager service, 21
metric store, 24
Metric Studio, 16
Microsoft .NET Framework, 17, 32, 50
Microsoft Office
Cognos 8 report data, 17
Cognos 8 report data in workbooks and presentations, 50
report data service, 22
migration
from other Cognos products to Cognos 8, 64
Migration service, 21
mobile devices
using to access reports, 67
modeling, 17, 18
and Cognos 8 performance, 88
databases, 48, 50
metadata, 48, 50
packages, 48
users, 48, 50
models, 48
creating, 48
Framework Manager, 48, 50
publishing, 48
monitor service, 21
multilingual
Map Manager, 104
multilingual reporting
configuring, 46

N

namespaces
Active Directory, 123
Cognos, 123
LDAP, 123
Series 7, 127
Sun Java System, 123

network
securing, 118

O

OLAP, 17
operating system
securing, 114
organizational units (OUs), 126

P

packages
creating, 48
Framework Manager, 48
parameter signing, 107
PDF
report compression, 24
running reports, 36, 38
viewing reports, 36
PDF rendering, 94
performance
application complexity, 72
dispatch times, 28
estimating load distribution, 71
planning, 69
performance metrics, 85
performance tuning, 85
permissions, 109
planning
availability, 81
checklist, 53
configuration, 53
implementation, 44, 53
installation, 53
performance, 69
planning data service, 21
planning job service, 21
planning Web service, 21
plannning administration console service, 21
plug-ins, 14
portal pages, 41
portal services, 14
portlets, 41
port usage, 33
PowerCubes
access in Cognos 8, 66
combining cubes from multiple locales, 104
conversion from Cognos Series 7, 104
language restrictions, 101
requirements for successful language conversion, 66
securing, 127
PowerPlay
considerations for upgrading to Cognos 8, 63
migrating PowerPlay Web reports to Cognos 8, 65
PowerPlay Web
requirements to upgrade reports to Cognos 8, 64
PowerPoint
See Microsoft Office, 17
presentations
using Cognos 8 data in Microsoft Office PowerPoint, 17
presentation service, 22
printing copyright material, 9
process capacity setting, 89
processing log messages, 28
product locales, 98, 100
prompts, 88

Q

query processing types, 88
Query Studio, 16, 49
queue metrics, 85
quick tours
using, 9

R

related documentation, 7
report bursting, 93
report data
using in Microsoft Office, 17, 50
report data service, 22
tuning, 90
ReportNet
requirements to upgrade to Cognos 8, 63
upgrading, 63
reports
bursting, 71, 93
creating, 49
multilingual, 104
running, 36
scheduling, 38, 71, 92

viewing, 36
report service metrics, 85
report services, 22
scalability, 80
tuning, 90
Report Studio, 16
report types
capacity planning, 70
request affinity, 78
requests
distributing, 28
flow processing, 33
managing, 28
requirements
modeling, 48, 50
robustness, *See* availability
roles, 110
securing Cognos Connection, 124
routers
using, 77
rsvpproperties.xml files, 96
run locale, 99
running
analysis, 36
HTML reports, 36, 37
reports, 36

S

scalability, 69, 75
Cognos 8 gateway, 75
Cognos 8 server, 80
Content Manager, 80
planning, 75
Web server, 75
searching Cognos 8 BI content, 67
SecureError, 107
secure logging, 107
secure sockets layer, 110
secure sockets layer, *See* SSL
securing
Cognos Connection, 123, 124, 126
content store, 128
data source signons, 127
network, 118
operating system, 114
PowerCubes, 127
temporary files, 122
Web servers, 118
security
audit, 128
authentication providers, 108
best practices, 113
Cognos 8, 107, 110
configuration, 46
Content Manager, 109
keys,, 110
See cryptographic keys
Series 7 namespace, 127
Series 7 PowerCubes
requirements for successful language conversion, 66
server
locales, 98
server affinity, 80
server metrics, 85
service request metrics, 85
services
agent, 20
authorization, 109
batch report, 20
Cognos 8, 22
Cognos Content Database, 24
Content Manager, 20, 22
data integration, 20
delivery, 20
event management, 20
job, 20
load balancing, 28
log, 21
Metrics Manager, 21
Migration, 21
monitor, 21
planning data, 21
presentation, 22
report, 22
report data, 22
scalability, 80
system, 22
services metrics, 85
session affinity, 79
session metrics, 85
signing key pair, 110
single signon, 109

sizing the content store, 73
SSL
application servers, 121
enabling, 121
enabling on Web servers, 118
SSL, *See* secure sockets layer
standby
Content Manager, 22
standby Content Manager, 19, 80
startup configuration, 45
files, 45
Sun Java System directory server, 123
system metrics, 85
system service, 22

T

temporary files
securing, 122
thresholds, metrics, 85
tiers
applications, 19
data, 24
Web server, 18
Transformer, 17
data access in Cognos 8, 66
troubleshooting
logging, 28
tuning
application servers, 87
Cognos 8, 85
databases, 87
dispatchers, 89
report services, 90

U

UNIX servers
fonts, 99
Upfront
migrating content to Cognos 8, 65
upgrading
from other Cognos products to Cognos 8, 63
user community
size, 70
user interfaces, 13
user load
estimating, 70
user locale, 98, 99
users, 109
active, 70
concurrent, 70
named, 70

V

viewing
analysis, 36
HTML reports, 36
PDF reports, 36

W

Web-based user interfaces, 14
Web browsers
configuring, 46
Web portal, 14
Web servers, 61
Apache, 118
enabling SSL, 118
IIS, 118
scalability, 75
securing, 118
tuning, 88
Web server tier, 18
Windows-based user interfaces, 17
workbooks
using Cognos 8 data in Microsoft Office Excel, 17
workflow, 43

X

XML configuration files, 45
XML support, 24

Y

Year, in dates, 103